



#y
S&H Form: (2/01)

Attorney Docket No. 1081.1118

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Ikuya MORIKAWA, et al.

Application No.: 09/853,782

Group Art Unit: Unassigned

Filed: May 14, 2001

Examiner: To Be Assigned

For: COMMUNICATION SETTING MANAGEMENT SYSTEM

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-145646

Filed: May 17, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 7/12/01

By: 

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 5月17日

出 願 番 号

Application Number:

特願2000-145646

出 願 人
Applicant(s):

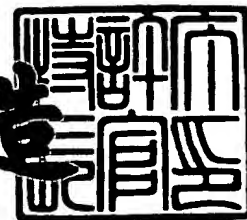
富士通株式会社

ゲーエムデー フォルシュンクスツェントルム インフォル
マチオンテクニック ゲーエムペーハー

2001年 5月11日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3040185

【書類名】 特許願

【整理番号】 0051009

【提出日】 平成12年 5月17日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 H04M 11/00

【発明の名称】 通信設定管理システム

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 森川 郁也

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 箕浦 真

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 福田 健一

【発明者】

【住所又は居所】 ドイツ連邦共和国 D-64295 ダルムシュタット
ラインストラッセ 75 ゲーエムデー フォルシュ
ンクスツェントルム インフォルマチオンテクニク
ゲーエムベーハー内

【氏名】 エリザベス ギースラー

【発明者】

【住所又は居所】 ドイツ連邦共和国 D-64295 ダルムシュタット
ラインストラッセ 75 ゲーエムデー フォルシュ
ンクスツェントルム インフォルマチオンテクニク

ゲーエムベーハー内
【氏名】 オラフ ヘンニガー
【発明者】
【住所又は居所】 ドイツ連邦共和国 D - 6 4 2 9 5 ダルムシュタット
ラインストラッセ 7 5 ゲーエムデー フォルシュ
ンクスツェントルム インフォルマチオンテクニク
ゲーエムベーハー内
【氏名】 ライナー プリノース
【発明者】
【住所又は居所】 ドイツ連邦共和国 D - 6 4 2 9 5 ダルムシュタット
ラインストラッセ 7 5 ゲーエムデー フォルシュ
ンクスツェントルム インフォルマチオンテクニク
ゲーエムベーハー内
【氏名】 トーマス シュレーダー
【特許出願人】
【識別番号】 000005223
【氏名又は名称】 富士通株式会社
【特許出願人】
【住所又は居所】 ドイツ連邦共和国 D - 5 3 7 5 7 サンクト オーガ
スティン
【住所又は居所原語表記】 D-53757 Sankt Augustin, Germany
【氏名又は名称】 ゲーエムデー フォルシュンクスツェントルム インフ
ォルマチオンテクニク ゲーエムベーハー
【氏名又は名称原語表記】 GMD-Forschungszentrum Informationstechnik
GmbH
【代理人】
【識別番号】 100094514
【弁理士】
【氏名又は名称】 林 恒▲徳▼

【代理人】

【識別番号】 100094525

【弁理士】

【氏名又は名称】 土井 健二

【手数料の表示】

【予納台帳番号】 030708

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704944

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信設定管理システム

【特許請求の範囲】

【請求項 1】 複数の通信実体（エンティティ）に対して通信の特性を定めた設定を配布する通信設定管理システムであって、

前記通信エンティティの具体的な設定方法の情報を参照して、該通信エンティティに対し設定する内容を纏めた設定テンプレートを、入力又は編集する設定テンプレート入力・編集手段と、

該設定テンプレート入力・編集手段により入力又は編集された設定テンプレートを蓄積する設定テンプレート蓄積手段と、

どのような属性を持った通信にどの設定テンプレートを適用すべきかの規則を記した適用規則を入力又は編集する適用規則入力・編集手段と、

該適用規則入力・編集手段により入力又は編集された適用規則を蓄積する適用規則蓄積手段と、

設定を配布する先の通信エンティティの属性に従って、前記適用規則蓄積手段から該当する適用規則を選び、該適用規則で指定される設定テンプレート名を有する設定テンプレートを前記設定テンプレート蓄積手段から読み出し、該読み出された設定テンプレートを前記通信エンティティに配布を行う検索・応答機能手段を備える

ことを特徴とする通信設定管理システム。

【請求項 2】 請求項 1 において、

さらに定義済みの設定テンプレート群を前記設定テンプレート蓄積手段に一括して入力する設定テンプレート一括入力手段を備えることを特徴とする通信設定管理システム。

【請求項 3】 それぞれ少なくとも 1 つの通信エンティティを有する複数の管理ドメインがネットワークを介して存在し、

該複数の管理ドメインの各々に配置される一つの通信設定管理装置を有し、

異なる管理ドメインに属する通信エンティティ間の通信に対し、該当する管理ドメインに配置される通信設定管理装置は、それぞれの管理ドメイン毎に異なる

通信特性の設定を与え、該設定を該当する管理ドメイン毎に管理することを特徴とする通信設定管理システム。

【請求項 4】請求項 3 において、前記通信設定管理装置は、

前記通信エンティティの具体的な設定方法の情報を参照して、該通信エンティティに対し設定する内容を纏めた設定テンプレートを、入力又は編集する設定テンプレート入力・編集手段と、

該設定テンプレート入力・編集手段により入力又は編集された設定テンプレートを蓄積する設定テンプレート蓄積手段と、

どのような属性を持った通信にどの設定テンプレートを適用すべきかの規則を記した適用規則を入力又は編集する適用規則入力・編集手段と、

該適用規則入力・編集手段により入力又は編集された適用規則を蓄積する適用規則蓄積手段と、

設定を配布する先の通信エンティティの属性に従って、前記適用規則蓄積手段から該当する適用規則を選び、該適用規則で指定される設定テンプレート名を有する設定テンプレートを前記設定テンプレート蓄積手段から読み出し、該読み出された設定テンプレートを前記通信エンティティに配布を行う検索・応答機能手段を

備えることを特徴とする通信設定管理システム。

【請求項 5】請求項 4 において、

さらに、他の管理ドメインに配置される通信設定管理装置と相互に情報を交換し、該情報と自管理ドメインの設定テンプレート及び適用規則との矛盾を検知する矛盾検出機能部を有することを特徴とする通信設定管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信実体（以下通信エンティティという）間で通信を行う際に、どのような通信にどのような特性を与えるかを定めた通信設定を一括して管理するための通信設定管理システムに関する。

【0002】

【従来の技術】

近年のネットワークの発展により、非常に多くのコンピュータや通信機器及び、オブジェクト指向等で実現されるソフトウェア部品などの通信実体（通信エンティティ）が有線あるいは無線のネットワークに接続され、相互間で様々な通信を行うようになっている。

【0003】

ここで通信実体即ち、通信エンティティとは、通信機能を有したコンピュータ、ルータなどの通信ハードウェア機器及び、オブジェクト指向等で実現されるソフトウェア部品を指す。また、通信の特性とは通信の速度や手順、セキュリティの程度や質などを指す。そして、通信設定とは通信の速度や質を指示するための処理手順、暗号アルゴリズム、暗号鍵の長さなどのパラメータを指す。

【0004】

上記のネットワークに接続された通信エンティティ間の通信では通信の特性を管理してネットワークの効率的な利用や適切なセキュリティの適用を行うことが望まれている。

【0005】

このための一提案として、例えば特開平6-6347号公報に記載のセキュリティ管理システムでは複数の通信機器にセキュリティに関する設定を分配するシステムが開示されている。

【0006】

このような場合には、通信の属性によって通信の特性を割り当てる。すなわち、通信設定を割り当てるのが一般的である。ここで通信の属性としては、通信の発信者（ユーザ名、ホスト名、ポート番号等）、受信者（ユーザ名、ホスト名、ポート番号、サービスの呼称、ファイル名等）、通信の種類（要求の内容、引数等）等が挙げられる。

【0007】

このような通信の属性に対し、それぞれどのような通信の設定を割り当てるかという規則を適用規則と呼び、このような通信の設定と適用規則を併せてポリシーと呼ぶ。

【 0 0 0 8 】

このような通信の設定を管理する仕組みとして図 1 に示すように第 1 の従来技術では設定レベルという概念を用いていた。図 1 において、ネットワークに接続される複数の通信エンティティ $2_1 \sim 2_n$ に対し、通信の設定を行う通信設定管理装置 1 が示される。

【 0 0 0 9 】

ここで、通信設定管理装置 1 は、適用規則入力・編集手段 1 0 0、適用規則蓄積手段 1 0 1 及び検索・応答機能部 1 0 2 を有する。これら手段及び機能部はハードウェアとして構成され、あるいはソフトウェアで実現される。

【 0 0 1 0 】

かかる通信設定管理装置 1 に対し、設定レベル 2 0 0 が用意される。この設定レベル 2 0 0 は異なる設定内容を大雑把なレベルで表したものであり、それ自体は具体的な設定内容を表していない。

【 0 0 1 1 】

そのかわりに設定レベルと具体的な設定内容の対照情報 2 0 1 が別途用意されている。この対照情報 2 0 1 と与えられた設定レベル 2 0 0 に照らし合わせて通信エンティティ $2_1 \sim 2_n$ に具体的にどのような設定を行うかが決定される。

【 0 0 1 2 】

管理者は、この設定レベル 2 0 0 のみ、あるいは設定レベル 2 0 0 と対象情報 2 0 1 を照らし合わせて、各々の通信に設定レベルを割り当てる適用規則を適用規則入力・編集手段 1 0 0 を用いて記述する。記述された適用規則は、適用規則蓄積手段 1 0 1 に格納される。

【 0 0 1 3 】

そして、適時に適用規則蓄積手段 1 0 1 から検索・応答機能部 1 0 2 により適用規則を検索し、対応する通信エンティティ $2_1 \sim 2_n$ に設定とする。この場合、適用規則と設定レベルは区別されて扱われる。つまりポリシーは、適用規則と設定レベルに明確に分けられる。

【 0 0 1 4 】

第 2 の従来方法として、図 1 の例のような設定レベル 2 0 0 を用意せずに、管

理者が適用規則を記述する際に割り当てる設定内容を詳細設定入力・編集手段 1 0 3 を用いて具体的に記述することもできる。この場合には、管理者には具体的な設定内容（2 0 2）に関する詳しい知識が必須であり、適用規則と設定は区別されておらず不可分のものとして扱われる。つまり、ポリシーは適用規則と設定が入り混じったものである。

【0 0 1 5】

また、通信設定管理装置 1 の配置方法として、従来図 3 に示すように一つの目的・用途については一つの通信設定管理装置 1 が複数の通信エンティティを一括して設定管理していた。そして、図 3 において、通信に関する設定についても通信の両端の通信エンティティ 2_1 - 2_2 への単独の通信設定管理装置が設定を与えていた。

【0 0 1 6】

【発明が解決しようとする課題】

上記第 1 の従来技術では、対照情報 2 0 1 が管理者から隠蔽されている場合には、管理者には詳細な設定内容に関する高度の知識を必要としない。容易に入力・編集が可能であるが、逆に高度の知識を持っていた際に詳細な設定内容に踏み込んで入力・編集を行うことができない。

【0 0 1 7】

一方、第 1 の従来技術で対照情報が管理者に提供されている場合及び、上記第 2 の従来技術の場合は、管理者は高度の知識を用いてきめ細かな設定を行うことが可能であるが高度の知識を有しない管理者にとっては設定を行うことが困難である。

【0 0 1 8】

すなわち、高度の知識を有してきめ細かなポリシーを記述したい管理者の要求と高度の知識を持たずに容易にポリシーを記述したい管理者の要求を同時に満たすことができず、知識の異なる管理者間で管理を分担することができないという問題がある。

【0 0 1 9】

したがって、本発明の目的は、通信設定を多くの通信エンティティへ配布する

場合において、高度の知識を要するきめ細かな通信設定の記述と高度の知識を要さない容易な適用規則の記述が同時に実現できる通信設定管理システムを提供することにある。

【0020】

さらに本発明の目的は、各ドメイン毎に配置することにより、管理ドメイン毎の異なる設定を実現する際の管理を効率化できる通信設定管理システムを提供することにある。

【0021】

【課題を解決するための手段】

前記の課題を解決する本発明に従う通信設定管理システムは、複数の通信実体（エンティティ）に対して通信の特性を定めた設定を配布する通信設定管理システムであって、前記通信エンティティの具体的な設定方法の情報を参照して、前記通信エンティティに対し設定する内容を纏めた設定テンプレートを、入力又は編集する設定テンプレート入力・編集手段と、前記設定テンプレート入力・編集手段により入力又は編集された設定テンプレートを蓄積する設定テンプレート蓄積手段と、どのような属性を持った通信にどの設定テンプレートを適用すべきかの規則を記した適用規則を入力又は編集する適用規則入力・編集手段と、前記適用規則入力・編集手段により入力又は編集された適用規則を蓄積する適用規則蓄積手段と、設定を配布する先の通信エンティティの属性に従って、前記適用規則蓄積手段から該当する適用規則を選び、前記適用規則で指定される設定テンプレート名を有する設定テンプレートを前記設定テンプレート蓄積手段から読み出し、前記読み出された設定テンプレートを前記通信エンティティに配布を行う検索・応答機能手段を備えることを特徴とする。

【0022】

好ましい態様として、さらに定義済みの設定テンプレート群を前記設定テンプレート蓄積手段に一括して入力する設定テンプレート一括入力手段を備えることを特徴とする。

【0023】

さらに好ましい態様として、それぞれ少なくとも1つの通信エンティティを有

する複数の管理ドメインがネットワークを介して存在し、前記複数の管理ドメインの各々に配置される一つの通信設定管理装置を有する。そして、異なる管理ドメインに属する通信エンティティ間の通信に対し、該当する管理ドメインに配置される通信設定管理装置は、それぞれの管理ドメイン毎に異なる通信特性の設定を与え、前記設定を該当する管理ドメイン毎に管理することを特徴とする。

【 0 0 2 4 】

かかる態様に対し、更に好ましい態様として、他の管理ドメインに配置される通信設定管理装置と相互に情報を交換し、前記情報と自管理ドメインの設定テンプレート及び適用規則との矛盾を検知する矛盾検出機能部を有することを特徴とする。

【 0 0 2 5 】

また、好ましい態様として、前記矛盾検出機能部により前記適用規則により指定される設定テンプレートあるいは設定テンプレートの集合が一致しない矛盾が検出された時、前記矛盾を修正する矛盾修正機能部を更に有することを特徴とする。

【 0 0 2 6 】

本発明の特徴は、以下の図面を参照して説明される発明の実施の形態から更に明らかになる。

【 0 0 2 7 】

【発明の実施の形態】

以下本発明の実施の形態を、添付図面を参照して説明する。なお、図面は本発明の説明のためのものであり、従って本発明の保護の範囲はかかる図面に記載されたものに限定されるものではない。

【 0 0 2 8 】

図 4 は、本発明の通信設定管理システムの第 1 の実施例概念を説明する図である。図において、通信設定管理装置 1 は、適用規則蓄積手段 1 1、設定テンプレート蓄積手段 1 2、検索・応答機能部 1 3、適用規則入力・編集手段 1 4、設定テンプレート入力・編集手段 1 5 を有して構成される。これらの機能部及び手段に対応する機能は、先に説明したように、ハードウェア又はソフトウェアで実現

可能である。

【 0 0 2 9 】

設定テンプレートは、通信エンティティに渡す設定をひとまとめにして名前をつけたものである。設定テンプレート入力・編集手段 1 5 は、詳細設定入力・編集機能を有している。設定テンプレートは高度な知識を有する上級管理者 2 1 が各通信エンティティの具体的な設定方法の情報 2 0 を参照しながら、設定テンプレート入力・編集手段 1 5 を用いて入力し、あるいは編集して設定テンプレート蓄積手段 1 2 に格納される。

【 0 0 3 0 】

適用規則はどのような属性を持った通信にどの設定テンプレートを適用すべきかという規則を記したものである。すなわち適用規則は通信の属性と設定テンプレート名の組である。適用規則は通常の管理者 2 2 が適用規則入力・編集手段 1 4 を用いて入力あるいは編集する。

【 0 0 3 1 】

適用規則入力・編集手段 1 4 は設定テンプレート名読み出し機能を有しており、設定テンプレート蓄積手段 1 2 から設定テンプレートの名前の一覧を読み出して、管理者に提示し選択させる。

【 0 0 3 2 】

こうして入力あるいは編集された適用規則は適用規則蓄積手段 1 1 へ格納される。通信が発生し、通信エンティティ 2 へ設定を配布するときには、検索・応答機能部 1 3 が配布先の通信の属性に従って適用規則蓄積手段 1 1 から該当する適用規則を選び出し、そこに指定されている設定テンプレート名を持つ設定テンプレートを設定テンプレート蓄積手段 1 2 から読み出す。そしてこの設定テンプレートを配布先の通信エンティティへ配布する。

【 0 0 3 3 】

本実施例では、設定テンプレート蓄積手段 1 2 と設定テンプレート入力・編集手段 1 5 を設け、各通信エンティティの具体的な設定方法 2 0 から利用したい組み合わせを取り出して入力・編集し、蓄積しておく方法を用いている。

【 0 0 3 4 】

これにより、典型的な設定テンプレートに関しては、高度な知識を有する上級管理者 21 がこれらを入力しておく。これにより、通常の管理者 22 は各通信エンティティの具体的な設定方法に関する高度な知識を持たなくとも適用規則を容易に入力することができる。

【0035】

また具体的な設定方法に関する高度な知識を有する上級管理者 21 は、設定テンプレート入力・編集手段 15 を用いて、設定テンプレートの中の詳細な値まで検討し、入力あるいは編集することによりきめ細かな設定テンプレートを作ることができる。

【0036】

このように、管理者の知識に応じて、高度な知識を必要とせずに容易に設定を割り当てることと、高度な知識を用いてきめ細かな設定を割り当てることの両立が可能である。

【0037】

したがって、知識の異なる管理者 21, 22 間で管理業務を分担し効率良くポリシー(設定および適用規則)を管理することができる。

【0038】

ここで、上記図 4 の実施例構成において、設定テンプレート入力・編集手段 15 は、管理者 21 との対話的な入出力により設定テンプレートを閲覧・入力・編集するものであり、すでに定義済みの多くの設定テンプレートがデータとして用意されている場合には、対話的に入力するのは手間がかかり効率が悪い。

【0039】

すなわち、図 4 に示す実施例構成では、設定テンプレートの入力は設定テンプレート入力・編集手段 15 を介して行われるが、これは対話的に管理者 21 に入力・編集させることを目的としており、既に定義済みの設定テンプレート群がある場合には効率が悪かった。

【0040】

そこで、定義済みの設定テンプレート群を一括して入力することを可能とする通信設定管理システムが要求される。図 5 は、かかる要求に対応する実施例の概

念構成を示す図である。

【 0 0 4 1 】

図 5 の実施例構成の特徴は、図 4 の実施例構成の通信設定管理装置 1 に対し、定義済みの設定テンプレート群 2 3 を用意し、これを一括して受け付け、設定テンプレート蓄積手段 1 2 へ格納する設定テンプレート一括入力手段 1 6 が追加されている。

【 0 0 4 2 】

一括して定義済みの設定テンプレート群を受け取るための設定テンプレート一括入力手段 1 6 により管理者の人手を要さずに一括して定義済み設定テンプレート群 2 3 を設定テンプレート蓄積手段 1 2 へ入力できる。これにより効率良く定義済み設定テンプレート群 2 3 を入力でき、特に通信エンティティの設計者が新たに実装した機能に対応する設定テンプレート群を配布する際に有効である。

【 0 0 4 3 】

ここで、通信に関するポリシーでは、通信の両端で等しくなければいけないポリシーもあるが、必ずしも等しくなくてもよいポリシーも存在する。セキュリティを例にとれば、通信内容の暗号化をする場合には用いる暗号アルゴリズムの種類や鍵の長さは等しく設定されなければならないが、通信の監査のポリシー、たとえばログをとるかどうかの設定は等しい必要はない。

【 0 0 4 4 】

また通信の両端で適用規則を記述したい通信属性のパラメータが異なる。たとえば、クライアントのユーザがサーバにあるファイルへアクセスするような通信であれば、クライアント側ドメインではユーザという属性に対して適用規則を記述するのは容易である。しかし、目的のファイルという属性ではファイルに関する知識が少ないので記述しづらい。

【 0 0 4 5 】

一方、サーバ側ドメインではファイルという属性に対して適用規則を記述するのは容易だが、ユーザという属性に対してはユーザに関する知識が少ないので記述しづらい。このような場合には、サーバ側とクライアント側で異なる適用規則

を記述できることが望ましい。

【 0 0 4 6 】

以上の二例のような場合に、図 3 に示したように、通信設定管理装置 1 が一つしか存在しないと、両ドメインがそれぞれ異なる組織である時に、通信設定管理装置 1 を有さない組織は相手の組織へポリシーの変更を依頼せねばならず、手間がかかり効率が悪い。

【 0 0 4 7 】

かかる問題を解決する本発明に従う構成として、図 6 に通信設定管理装置 1 の配置方法を示す。

【 0 0 4 8 】

図 6 において、通信エンティティ 2 は、管理ドメイン 4 にあり、複数の管理ドメイン 4 間はネットワーク 3 で接続されている。そして、管理ドメイン 4 毎に一つの通信設定管理装置 1 が配置され、各通信設定管理装置 1 が対応する管理ドメイン 4 内の通信エンティティ 2 へ設定を供給（フィード）する。

【 0 0 4 9 】

ここで、管理ドメイン 4 はどのような領域に対応していても構わないが、通信エンティティ 2 を管理する組織毎に区切るのが一般的である。図示されていないが、管理ドメイン 4 内の通信エンティティ 2 は互いに接続されており、また管理ドメイン 4 間をつなぐネットワーク 3 へも接続されているものとする。

【 0 0 5 0 】

このように、管理ドメイン 4 毎に通信設定管理装置 1 を配置することにより、通信の両端で異なっても構わない、あるいは異なっていた方が都合のよい通信のポリシー（設定テンプレートおよび適用規則）を、各ドメインごとに記述し、管理することが可能となる。これにより、通信設定管理装置 1 が一つだけである場合に発生する、相手組織への変更依頼などの非効率が解消できる。

【 0 0 5 1 】

ここで、図 6 に示す構成では、管理ドメインごとに通信設定管理装置が配置されるので、通信の両端で等しくなければならない設定を異なる設定内容で記述してしまう可能性がある。

【 0 0 5 2 】

たとえば、ある通信に対して両端で異なる暗号アルゴリズムを適用するようなポリシー（設定あるいは適用規則）が入力されると、実際にその通信が発生したときに暗号アルゴリズムの相違のため通信が達成できない。

【 0 0 5 3 】

したがって、かかる問題を解決するための実施例構成として、図 7 にその概念構成を示す。すなわち、図 7 の実施例構成は、図 6 の構成において、通信設定管理装置 1 が、ドメイン 4 毎に配置された場合に、異なるドメインの通信設定管理装置 1 との間で生じる設定や適用規則の矛盾を解決することが可能な通信設定管理システムに関するものである。

【 0 0 5 4 】

図 7 の実施例構成において、図 4 の実施例構成における通信設定管理装置 1 に対し、異なるドメインの通信設定管理装置 1 と互いに情報を交換し（23）、その情報を用いて設定や適用規則の矛盾を検出する矛盾検出機能部 17 が追加されている。これにより通信設定管理装置 1 において、他のドメインの通信設定管理装置 1 に適用される異なる設定テンプレートが指定されることに起因する矛盾を解消することができる。

【 0 0 5 5 】

すなわち、通信設定管理装置 1 が前記の矛盾検出機能部 17 を有することにより、通信相手の管理ドメインの通信設定管理装置 1 との間でのポリシー（設定テンプレートおよび適用規則）の矛盾を検出することができる。これにより、矛盾した設定テンプレートを通信エンティティに与えてしまい、その結果通信エンティティが相手との通信に失敗するなどの問題を回避することができる。

【 0 0 5 6 】

ここで、図 7 の実施例構成において、ポリシー（設定や適用規則）の矛盾を検出できるが、検出した矛盾を設定や適用規則を入力し直したり編集したりすることによって修正するのでは、手間がかかり非効率的である。

【 0 0 5 7 】

矛盾の原因の一つとして、適用規則に従った結果選ばれた設定テンプレートあ

るいは設定テンプレートの集合が異なっていることが考えられる。かかる点を考慮した実施例構成の概念図を図 8 に示す。

【 0 0 5 8 】

図 8 の実施例構成において、通信設定管理装置 1 に対し、更に矛盾修正機能部 1 8 を備えている。矛盾検出機能部 1 8 は矛盾を検出すると、矛盾修正機能部 1 7 へ修正を要求する。

【 0 0 5 9 】

矛盾修正機能部 1 7 は、もし検出された矛盾が適用規則が異なる設定テンプレートあるいは設定テンプレートの集合を指定していることに起因していて、しかもその相違が図示されない所与の規則によって修正可能な場合には、この矛盾を修正可能なものと見なす。

【 0 0 6 0 】

修正可能と見なされた矛盾をどのように扱うかは本発明では特に規定しないが、たとえば修正可能なので矛盾と見なさずに受け入れる、あるいは修正した結果を新たな適用規則として適用規則蓄積手段 1 4 へ格納する、などが考えられる。

【 0 0 6 1 】

このように、図 8 の実施例構成では、矛盾修正機能部 1 8 が前記の働きをすることにより、適用規則が指定する設定テンプレートが通信相手と異なっている、あるいは設定テンプレートの集合が完全に一致しないなどに起因する矛盾を修正可能と見なすことができ、あるいは実際に修正を施すこともできる。

【 0 0 6 2 】

これにより上記の原因に起因する矛盾を管理者 2 1、2 2 の人手による修正を要せずに自動的に回避・修正することが可能となる。

【 0 0 6 3 】

以下に、上記の実施例概念を適用し、通信設定管理システムを通信のセキュリティ設定の管理に用いた場合の具体的な実施例を説明する。

【 0 0 6 4 】

図 9 は、上記の実施例概念を総合して適用し、通信設定管理システムを通信のセキュリティ設定の管理に用いた場合の具体的な実施例を示す図であり、通信設

定管理装置 1 とそれを備えたシステム全体の構成例を示す。

【 0 0 6 5 】

各通信エンティティの具体的な設定方法に関する情報 2 0 は通信設定管理装置 1 の内部に保持される必要はないが、この実施例では図のように通信設定管理装置 1 の内部に保持している。

【 0 0 6 6 】

この実施例では、個々の通信を区別するための属性を次の三つのパラメータから成るものとする。すなわち、主体 (subject)、動作 (action)、客体 (object) である。

【 0 0 6 7 】

以下では、主体はユーザ名、客体はサーバの種類、及び動作は客体のサーバに対する処理であって、読み出し (read) と書込み (write) から成るものとする。

【 0 0 6 8 】

図 1 0 は、通信エンティティの具体的な設定方法の情報 2 0 の構成例である。この情報 2 0 は、情報テーブル化され、通信エンティティがサポートしている可能性のあるセキュリティ機能の設定の方法を示している。そして、情報テーブルにある文字列を受け取ると通信エンティティは対応するセキュリティ機能を適用するものとする。

【 0 0 6 9 】

このセキュリティ機能は、この実施例では認証 2 0 0、秘匿 2 0 1、ログ記録 (監査) 2 0 2 の三つの分野に分けられている。

【 0 0 7 0 】

さらに、認証 2 0 0 には R S A アルゴリズムを 5 1 2 ビットの鍵、1 0 2 4 ビットの鍵及び 2 0 4 8 ビットの鍵で利用する設定、および認証なしの 4 種の選択肢が示されている。

【 0 0 7 1 】

秘匿 2 0 1 には D E S 暗号と Triple D E S 暗号、および秘匿なしの三つの選択肢が示されている。また、ログ記録 2 0 2 には単純にありとなしの二つの選択肢

が示されている。

【 0 0 7 2 】

図 1 1 は設定テンプレート蓄積手段 1 2 に格納されている設定テンプレートの構成例である。設定テンプレートは、設定テンプレート名 2 1 0 と、上記の通信エンティティの具体的な設定方法の情報 2 0 から求められる具体的な設定内容 2 1 1 の組から成る。図 1 1 に示す例では補助的な情報としてコメント 2 1 2 も加えられている。

【 0 0 7 3 】

図 1 2 は適用規則蓄積手段 1 1 に格納されている適用規則の構成例である。主体(Subject) 2 2 0 として指定されているAdmin, Customer, Userは個々のユーザ名ではなくそれぞれユーザの属するグループ名であり、順に管理者グループ、顧客グループ、一般ユーザグループを表す。

【 0 0 7 4 】

ユーザのグループに対する所属関係の情報は図示されない蓄積手段によって管理ドメインごとに蓄積されており、管理者 2 1, 2 2 や通信設定管理装置 1 は自由に得ることができるものとする。

【 0 0 7 5 】

次に、図 9 の実施例構成において、図 4 の実施例概念を実現する動作を説明する。第一の手順は、設定テンプレートの入力である。

【 0 0 7 6 】

図 1 3 は、設定の方法(この例ではセキュリティ設定の方法)について高度な知識を有する上級管理者 2 1 が、設定テンプレート入力・編集手段 1 5 を用いて、設定テンプレートを入力する際に示される画面の例である。

【 0 0 7 7 】

図では「T 0 4」という名の新たな設定テンプレートを追加しようとしている。設定内容 2 1 1 の認証 2 0 0 の部分について、4 つの選択肢が示されている。これらの選択肢は、図 1 0 に示した通信エンティティの具体的な設定方法の情報 2 0 から得られたものである。

【 0 0 7 8 】

上級管理者 2 1 はこの情報 2 0 を参照してどの認証方法がふさわしいかを判断し入力する。このように入力された設定テンプレートは、設定テンプレート入力・編集手段 1 5 により設定テンプレート蓄積手段 1 2 へ格納される。

【 0 0 7 9 】

第二の手順は適用規則の入力である。図 1 4 は、高度な知識を有さない一般の管理者 2 2 が、通用規則入力・編集手段 1 4 を用いて、適用規則を入力する際に示される画面の例である。

【 0 0 8 0 】

図 1 4 では関係会社の人間(Ex#staffグループ)が設計図面サーバから読み出す際のセキュリティ設定を記述しようとしている。割り当てられた設定テンプレートについて設定テンプレート蓄積手段 1 2 から読み出される 5 つの設定テンプレート名(T01,T02,T03,T04)とそれぞれに対応するコメントが、選択肢として提示されている。これらは図 1 1 に示した設定テンプレート蓄積手段 1 2 の内容から得られたものであり、このように入力されて適用規則は適用規則蓄積手段 1 1 に格納される。

【 0 0 8 1 】

図 1 5 は、上記の二つの手順を経て用意された情報を基に、通信エンティティ 2 に設定テンプレートを配布する実施例動作フローである。通常、検索・応答機能部 1 3 は通信エンティティ 2 からの要求を待っている(3 0 0)。

【 0 0 8 2 】

通信エンティティ 2 は、ユーザからの指令で通信を開始する際に、その通信にどのような設定を適用するべきであるかを知るために、通信設定管理装置 1 に要求を出す。この時、通信の属性である主体 2 2 0 のユーザ名、客体 2 2 2 のサーバ名、及び希望する動作 2 2 1 を通信設定管理装置 1 へ知らせる。ここでは順に「yamada」、「人事情報サーバ」、「read」であったとする。

【 0 0 8 3 】

通信設定管理装置 1 は、通信エンティティ 2 からの要求を受信する(3 0 0 - Y E S)と、要求を解析し、前記の属性の三項目(2 2 0, 2 2 1, 2 2 2)を得る(3 0 2)。

【 0 0 8 4 】

次にこの属性と合致する適合規則を適用規則蓄積手段 1 1 から検索する（3 0 3）。この時、この例では適用規則の主体 2 2 0 欄はグループ名で記載されているので、図示されない蓄積手段よりユーザ名が属するグループ名を得る必要がある。

【 0 0 8 5 】

ここでは、ユーザ「yamada」はグループ「User」のみに属していたとする。すると、この属性に合致する適用規則は図 1 2 における第 6 行目の規則であるから「T 0 2」という名の設定テンプレートを適用すべきことが分かる。

【 0 0 8 6 】

もし、ここで該当する適用規則が見つからなければ（3 0 4 - N O）、エラーが有ったことを通信エンティティ 2 へ返答し、要求待ち状態へ戻る（3 0 5）。

【 0 0 8 7 】

この例のように見つかった場合には、検索・応答機能部 1 3 は「T 0 2」という名の設定テンプレートを設定テンプレート蓄積手段 1 2 から検索して取得する（3 0 6）。これを通信エンティティ 2 へ返す（3 0 7）。そして、再び要求を待つ状態に戻る。

【 0 0 8 8 】

通信エンティティ 2 は受け取った設定テンプレートに従って通信の特性を設定する。すなわち、この例では図 1 1 から R S A アルゴリズムで 5 1 2 ビットの鍵を用いて認証（2 0 0）を行い、通信の内容は D E S アルゴリズムで暗号秘匿化（2 0 1）し、通信の記録をログ（2 0 2）に残すように設定を行う。

【 0 0 8 9 】

なお、通信エンティティ 2 がどのように設定テンプレートの解釈を行い、設定を行うかは本発明では特に規定されるものではない。

【 0 0 9 0 】

次に図 9 の実施例構成において、図 5 の実施例概念を実現する動作を説明する。

【 0 0 9 1 】

ここで、ある組織に新たに R C 4 暗号アルゴリズムで秘匿を実現できる通信エンティティ 2 が導入されたものとする。この時そのような通信エンティティ 2 の設計者や、高度な知識を有する上級管理者 2 1 は図 1 6 A に示す設定テンプレート群 2 3 を用意し、これらをそれぞれ入力する代わりに、設定テンプレート一括入力手段 1 6 を用いて容易に設定テンプレート蓄積手段 1 2 に追加することが可能である。

【 0 0 9 2 】

設定テンプレート蓄積手段 1 2 は、与えられた定義済みの設定テンプレート群 2 3 に対し、含まれるそれぞれの設定テンプレートが、図 1 6 B に示される許容される設定内容 2 1 1 の情報に反しないかを確認する。問題がなければ次々に設定テンプレート蓄積手段 1 2 に追加していく。設定内容 2 1 1 の情報に反していたものは一旦全てを受け取った後で、まとめて違反を入力者に通知する。

【 0 0 9 3 】

次に、具体的実施例 2 として、異なる組織を管理ドメイン 4 とした場合の、図 6 乃至図 7 に関する構成例や動作を示す。

【 0 0 9 4 】

図 1 7 は図 6 に示す通信設定管理装置 1 の配置方法の具体例である。組織 A, B をまたぐ通信が発生した際には、両端の通信エンティティ $2_1 - 2_2$ の属する管理ドメイン 4 の通信設定管理装置 1 がそれぞれ設定をフィードする。管理ドメイン 4 は組織 A, B ごとに分けられたものであり、ここではそれぞれが企業であるものとする。

【 0 0 9 5 】

各々の通信設定管理装置 1 の内部はすでに述べた実施例と同じで図 9 の構成を有するものとする。また、組織 A および B の通信設定管理装置 1 は、図 1 8 に示す設定テンプレートを共有し、それぞれ設定テンプレート蓄積手段 1 2 に格納しているものとする。

【 0 0 9 6 】

図 1 9 A, 1 9 B はそれぞれ組織 A および B の適用規則である。組織 B では、すでに図に示した適用規則を通信設定管理装置 1 の適用規則蓄積手段 1 1 に格納

しているものとする。

【 0 0 9 7 】

この場合、組織 A で図に示した適用規則 3 1，3 2 を入力する場合を考える。
なお、適用規則は、番号が若いもの程優先順位が高く、即ち検索時には上から順に検索して最初に合致したものを適用するものとする。

【 0 0 9 8 】

図 6 において説明したように、管理ドメイン 4 ごとに通信設定管理装置 1 を配置する利点は、管理ドメイン 4 ごとに異なるポリシーを入力できることである。

【 0 0 9 9 】

たとえば、適用規則 3 1 を入力した場合、主体 2 2 0 が User グループ、客体 2 2 2 が一般サーバ、動作 2 2 1 が読み出しであるような通信に対して、組織 A では T 2 1、組織 B では T 2 2、と異なる設定テンプレートが割り当てられることになる。

【 0 1 0 0 】

しかし、図 1 8 によれば、テンプレート T 2 1 と T 2 2 の相違はログ記録 2 0 2 の有無だけである。ログ記録 2 0 2 は通信の両端で等しくなくてもよい。すなわち、一方でログを記録し、もう一方ではログを記録しなくても構わないのであるから、このような設定は有効である。

【 0 1 0 1 】

また、適用規則 3 2 を入力した場合、組織 A では User というグループ名で、組織 B では Section A というグループ名で割り当てられるが、組織 A では、一般ユーザグループ User、管理者グループ Admin、といった区分でユーザを管理している。一方、組織 B では、部署 A Section A、部署 B Section B といった区分でユーザを管理しているのであれば、Section A、Section B のように適用規則を記述する方が容易である。

【 0 1 0 2 】

ただし、User グループと Section A グループに重なりがあった場合、即ち両方のグループに属するユーザがいた場合には、組織 A では T 2 3、組織 B では T 2 4 という異なる設定テンプレートが割り当てられる。このため、矛盾が生じる可

能性がある。

【0103】

このような矛盾を検出、あるいは回避・修正する図6乃至図8の具体例を以下に説明する。

【0104】

矛盾検出機能部17が他の管理ドメイン4と授受する情報の内容や情報を得た後、それを用いての具体的な矛盾検出アルゴリズムについては、通信の属性や適用規則の記述法などに依存するので、本発明では特に限定されない。

【0105】

ここでは単純にグループの帰属情報を用いてグループの重なりを調べ、設定テンプレート同士の矛盾あるいは同値関係は別途情報として与えられるような、簡単な矛盾検出法を例に説明する。なお、その他の矛盾検出法としては、上記特開平6-6347号公報に記載の方法などが挙げられる。

【0106】

図20は、矛盾検出の動作を説明する図である。適用規則31が入力される(300)と組織Aの通信設定管理装置1の矛盾検出機能部17は、組織Bの通信設定管理装置1へ適用規則の一覧とグループ所属情報を要求する(301)。

【0107】

組織Bの通信設定管理装置1はこの要求を受け、図18にある適用規則の一覧とグループ所属情報を返す(302)。次に、組織Aの矛盾検出機能部17は入力された適用規則と組織Bの適用規則の一つ一つを順に照合し、必要ならばグループ所属情報を用いて属性(この場合主体属性)に重なりがないかを検査しながら、矛盾の有無を検査していく(303)。

【0108】

ここではまず単純に設定テンプレート名が異なれば矛盾していると判断するものとする。適用規則31が入力されると、これを矛盾検出機能部17は組織Bの三つの適用規則と順に照合していくが、最初の適用規則との照合で、割り当てられる設定テンプレートが異なるにも関わらず、三つの属性が完全に一致していることがわかる。

【0109】

そこで、ここでいったんは矛盾と見なされることとなる。また適用規則32が入力されると、最初の適用規則とは矛盾しないが、二番目の適用規則との間で、まず割り当てられる設定テンプレートが異なるので矛盾の可能性があることがわかり、次に三つの属性のうち客体、動作の二つが一致しているので、残る主体のグループが重なりを持つかどうかの問題となる。

【0110】

そこで、組織Bのグループ所属情報と組織Aのグループ所属情報を照合し、UserグループとSection Aグループが重なりを持つかを検査する。重なりを持つなら、ここでいったんは矛盾と見なされる。

【0111】

もし矛盾の修正をしないのであれば、たとえば矛盾と見なされた適用規則を管理者へ報告し、再入力を促すことが出来る(304)。

【0112】

次に、前記のように検出された矛盾を修正する方法について述べる。図21は矛盾修正の動作例を説明する図である。この動作例では、矛盾修正機能部18は図示されていない二つの情報を有しているものとする。それは設定テンプレートの同値情報と優先情報である。これらの例を図22に示した。

【0113】

まず矛盾修正機能部18は矛盾を検出し(400)、検出された矛盾を同値情報と照合し、無視できないかを検査する(401)。同値情報とは異なる設定テンプレート名であっても、その相違は通信の両端で異なっても構わないものであるから、同値と見なしてよい設定テンプレートの組を示したものである。

【0114】

たとえば、適用規則31の入力では、T21とT22の設定テンプレートの相違が矛盾として検出されるが、これらの相違はログ記録の有無に関するもののみなので、同値情報にT21とT22は同値と見なしてよいと記されている(図22A参照)。そこでこの相違は矛盾ではないと見なすことになる。

【0115】

次に、矛盾修正機能部 1 8 は検出された矛盾を優先情報（図 2 2 B 参照）と照合し、優先順位によって修正できないか検査する。

【0 1 1 6】

優先情報とは異なる設定テンプレート間に優先順位があり、一方の設定テンプレートに修正して構わないような設定テンプレートの組を示したものである。

【0 1 1 7】

たとえば、適用規則 3 2 の入力では、前記のとおり User グループと Section A グループとの重なりにおいて一方で T 2 3、もう一方で T 2 4 が選ばれるという矛盾が生じる。

【0 1 1 8】

しかし、T 2 3 と T 2 4 の相違は暗号アルゴリズムの相違であり、より強力な暗号アルゴリズムを選択すれば済むのであれば、DES（T 2 3）より Triple DES（T 2 4）の方が強力であるので、T 2 3 を T 2 4 に修正することで矛盾を回避できる。

【0 1 1 9】

矛盾を修正する場合には、組織 B へ適用規則の変更を伝えねばならないが、このとき組織 A と B のどちらの適用規則が修正されるのかを判断する。先の例（図 2 2 B）では、修正される T 2 3 を割り当てていたのは組織 A の方なので、グループの重なり部分 5 0 0（グループの関係を示す図 2 3 を参照）では組織 A の適用規則 3 2 が修正されるべきである。

【0 1 2 0】

しかし、重ならない部分では組織 A の T 2 3 の割り当てが有効であるから、重なり部分が修正結果となり、その他の部分には影響を与えないよう、適用規則を挿入する位置の番号を決める（図 2 3 参照）。

【0 1 2 1】

この例の場合には、組織 A では番号 2 の前に組織 B の適用規則を追加し、組織 B では番号 2 の後ろに組織 A の適用規則を追加する必要がある。この判断結果を組織 B の通信設定管理装置の矛盾修正機能部へ伝え、自分は前記のように適用規則を適用規則蓄積手段へ追加する。

【 0 1 2 2 】

これにより、組織 A 及び B の適用規則蓄積手段 1 1 は図 2 4 のようになる。
 なお上記の実施例 2 では、グループ所属情報を用い、すべてのグループの構成員について重複がないかを調べる方式を用いているが、もしグループが互いに重なりを持たないように定義されていたり、重なりの有無を知る方法が別に用意されているのであれば、それらを用いて重複の検出を行っても構わない。

【 0 1 2 3 】

また、上の例では主体であるユーザのグループのみについて重複を検査しているが、E. Lupu and M. Sloman "Conflict Analysis for Management Policies" Fifth IFIP/IEEE に記載あるようにそれ以外の属性についても同様に検査することが可能である。

【 0 1 2 4 】

また、矛盾修正を設定テンプレートの同値情報と優先情報が別途用意されているものと見なして行っているが、矛盾を無視したり新たな設定テンプレートへ修正したりするための手段や必要な情報はこれに限らない。

【 0 1 2 5 】

(付記 1) 複数の通信実体 (エンティティ) に対して通信の特性を定めた設定を配布する通信設定管理システムであって、

前記通信エンティティの具体的な設定方法の情報を参照して、該通信エンティティに対し設定する内容を纏めた設定テンプレートを、入力又は編集する設定テンプレート入力・編集手段と、

該設定テンプレート入力・編集手段により入力又は編集された設定テンプレートを蓄積する設定テンプレート蓄積手段と、

どのような属性を持った通信にどの設定テンプレートを適用すべきかの規則を記した適用規則を入力又は編集する適用規則入力・編集手段と、

該適用規則入力・編集手段により入力又は編集された適用規則を蓄積する適用規則蓄積手段と、

設定を配布する先の通信エンティティの属性に従って、前記適用規則蓄積手段から該当する適用規則を選び、該適用規則で指定される設定テンプレート名を有

する設定テンプレートを前記設定テンプレート蓄積手段から読み出し、該読み出された設定テンプレートを前記通信エンティティに配布を行う検索・応答機能手段を備える

ことを特徴とする通信設定管理システム。

【 0 1 2 6 】

(付記 2) 付記 1 において、

さらに定義済みの設定テンプレート群を前記設定テンプレート蓄積手段に一括して入力する設定テンプレート一括入力手段を備えることを特徴とする通信設定管理システム。

【 0 1 2 7 】

(付記 3) それぞれ少なくとも 1 つの通信エンティティを有する複数の管理ドメインがネットワークを介して存在し、

該複数の管理ドメインの各々に配置される一つの通信設定管理装置を有し、

異なる管理ドメインに属する通信エンティティ間の通信に対し、該当する管理ドメインに配置される通信設定管理装置は、それぞれの管理ドメイン毎に異なる通信特性の設定を与え、該設定を該当する管理ドメイン毎に管理することを特徴とする通信設定管理システム。

【 0 1 2 8 】

(付記 4) 付記 3 において、前記通信設定管理装置は、

前記通信エンティティの具体的な設定方法の情報を参照して、該通信エンティティに対し設定する内容を纏めた設定テンプレートを、入力又は編集する設定テンプレート入力・編集手段と、

該設定テンプレート入力・編集手段により入力又は編集された設定テンプレートを蓄積する設定テンプレート蓄積手段と、

どのような属性を持った通信にどの設定テンプレートを適用すべきかの規則を記した適用規則を入力又は編集する適用規則入力・編集手段と、

該適用規則入力・編集手段により入力又は編集された適用規則を蓄積する適用規則蓄積手段と、

設定を配布する先の通信エンティティの属性に従って、前記適用規則蓄積手段

から該当する適用規則を選び、該適用規則で指定される設定テンプレート名を有する設定テンプレートを前記設定テンプレート蓄積手段から読み出し、該読み出された設定テンプレートを前記通信エンティティに配布を行う検索・応答機能手段を

備えることを特徴とする通信設定管理システム。

【0129】

（付記5）付記4において、

さらに、他の管理ドメインに配置される通信設定管理装置と相互に情報を交換し、該情報と自管理ドメインの設定テンプレート及び適用規則との矛盾を検知する矛盾検出機能部を有することを特徴とする通信設定管理システム。

【0130】

（付記6）付記5において、

前記矛盾検出機能部により前記適用規則により指定される設定テンプレートあるいは設定テンプレートの集合が一致しない矛盾が検出された時、

該矛盾を修正する矛盾修正機能部を更に有することを特徴とする通信設定管理システム。

【0131】

【発明の効果】

本発明によれば、通信設定を多くの通信エンティティへ配布する通信設定管理装置において、高度な知識を要するきめ細かな通信設定の記述と高度な知識を要さない容易な適用規則の記述が同時に実現でき、管理者の知識によって両者を使い分けることができる。

【0132】

また、通信設定管理装置を各管理ドメインごとに配置することにより、管理ドメインごとに異なる設定を実現する際の管理が効率化される。またその際に相手管理ドメインとの間で生じるポリシー（設定と適用規則）の矛盾を自動的に検出し、あるいは人手を介さずに自動的に修正することが可能となる。

【図面の簡単な説明】

【図1】

第 1 の従来技術を説明する図である。

【図 2】

第 2 の従来技術を説明する図である。

【図 3】

第 3 の従来技術を説明する図である。

【図 4】

本発明の第 1 の実施例構成を説明する図である。

【図 5】

本発明の第 2 の実施例構成を説明する図である。

【図 6】

本発明の第 3 の実施例構成を説明する図である。

【図 7】

本発明の第 4 の実施例構成を説明する図である。

【図 8】

本発明の第 5 の実施例構成を説明する図である。

【図 9】

本発明の上記第 1 の実施例における通信設定管理装置の具体的構成例ブロック図である。

【図 1 0】

本発明の上記第 1 の実施例における設定テンプレート蓄積手段に格納される設定テンプレートの例である。

【図 1 1】

本発明の上記第 1 の実施例における設定テンプレート蓄積手段に格納される設定テンプレートの他の例である。

【図 1 2】

本発明の上記第 1 の実施例における適用規則蓄積手段に格納される適用規則の例である。

【図 1 3】

本発明の上記第 1 の実施例における上級管理者に示される設定テンプレート入

力・編集の画面の例である。

【図 1 4】

本発明の上記第 1 の実施例における一般の管理者に示される適用規則入力・編集画面の例である。

【図 1 5】

本発明の上記第 1 の実施例における検索・応答機能部の動作説明図である。

【図 1 6】

本発明の上記第 1 の実施例における一括して追加される設定テンプレート群の例である。

【図 1 7】

本発明の上記第 2 の実施例における通信設定管理装置の配置の例である。

【図 1 8】

第 2 の実施例における組織 A 及び B の通信設定管理装置が共有している設定テンプレートの例である。

【図 1 9】

図 1 8 における組織 A 及び B の適用規則を示す図である。

【図 2 0】

矛盾検出機能の動作説明図である。

【図 2 1】

設定テンプレートの同値情報及び優先情報である。

【図 2 2】

矛盾修正の動作説明図である。

【図 2 3】

矛盾修正の概念図である。

【図 2 4】

矛盾修正後の適用規則である。

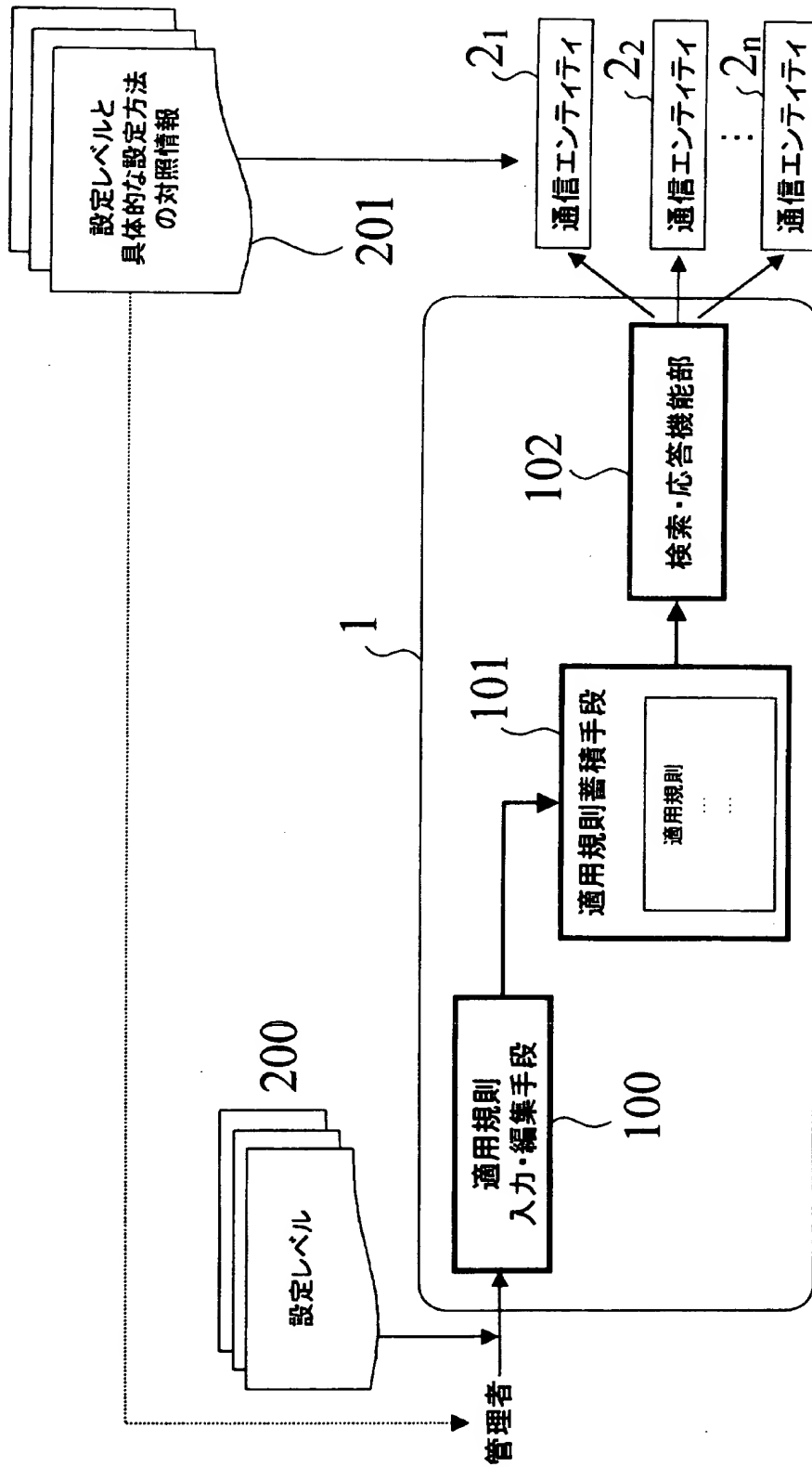
【符号の説明】

1 …通信設定管理装置、2 …通信エンティティ、3 …ネットワーク、4 …管理ドメイン、11 …適用規則蓄積手段、12 …設定テンプレート蓄積手段、13 …

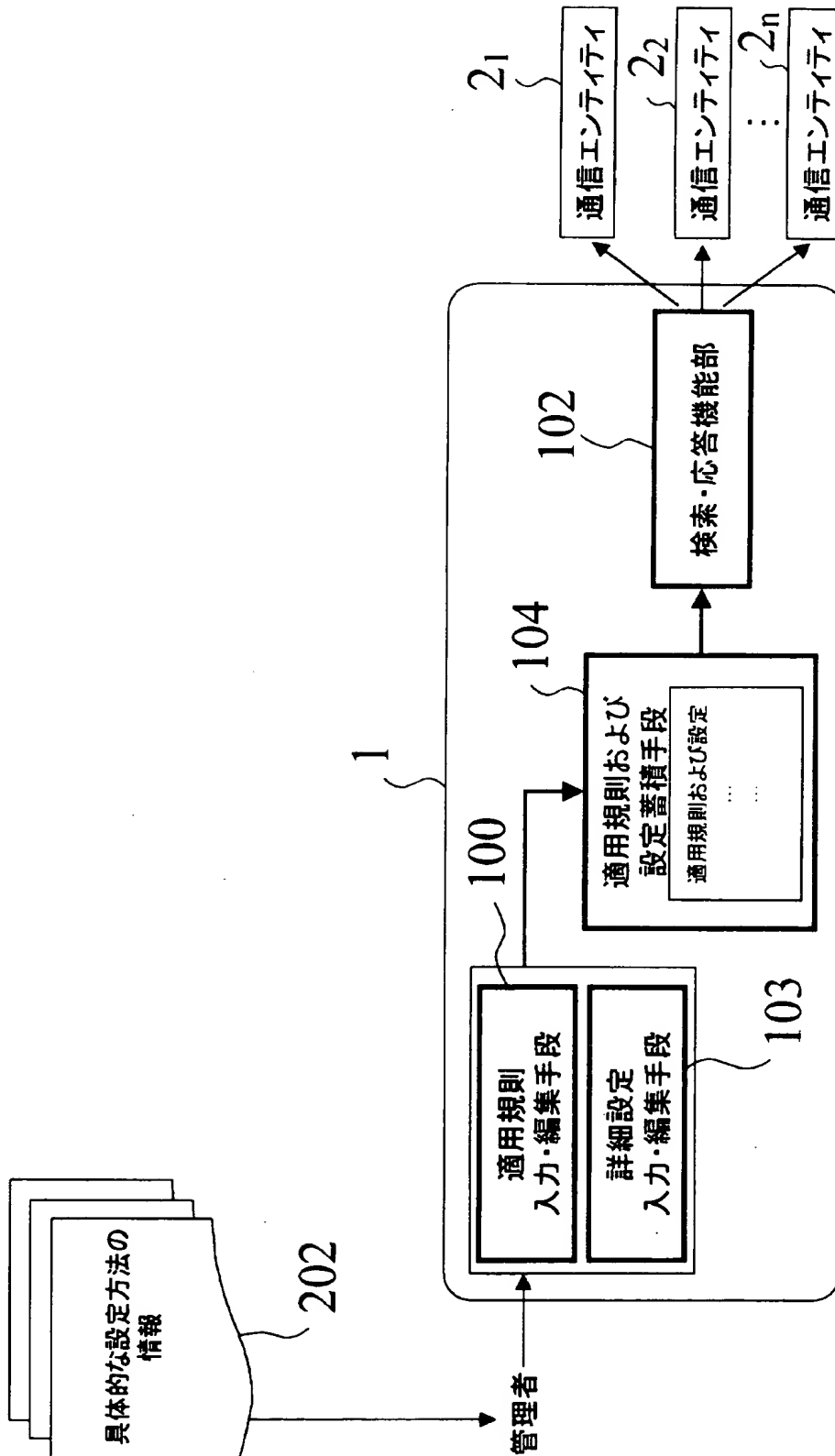
検索・応答検能部、14…適用規則入力・編集手段、15…設定テンプレート入力・編集手段、16…設定テンプレート一括入力手段、17…矛盾検出機能部、18…矛盾修正機能部、20…各通信エンティティの具体的な設定方法の情報、21…高度な知識を有する上級管理者、22…一般の管理者、23…定義済みの設定テンプレート群、31・32…組織Aの適用規則の例、41・42…組織Bの適用規則の例

【書類名】 図面

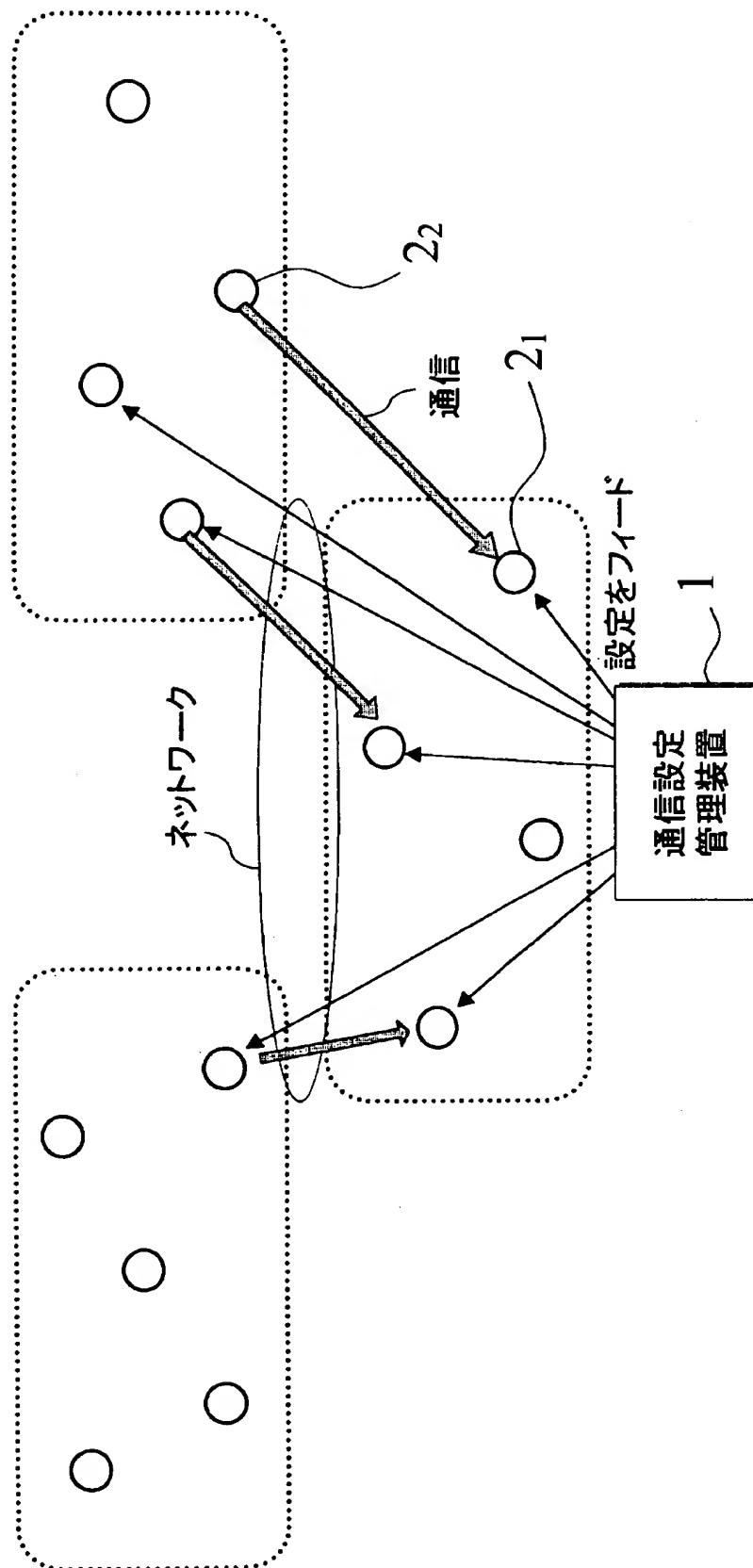
【図 1】



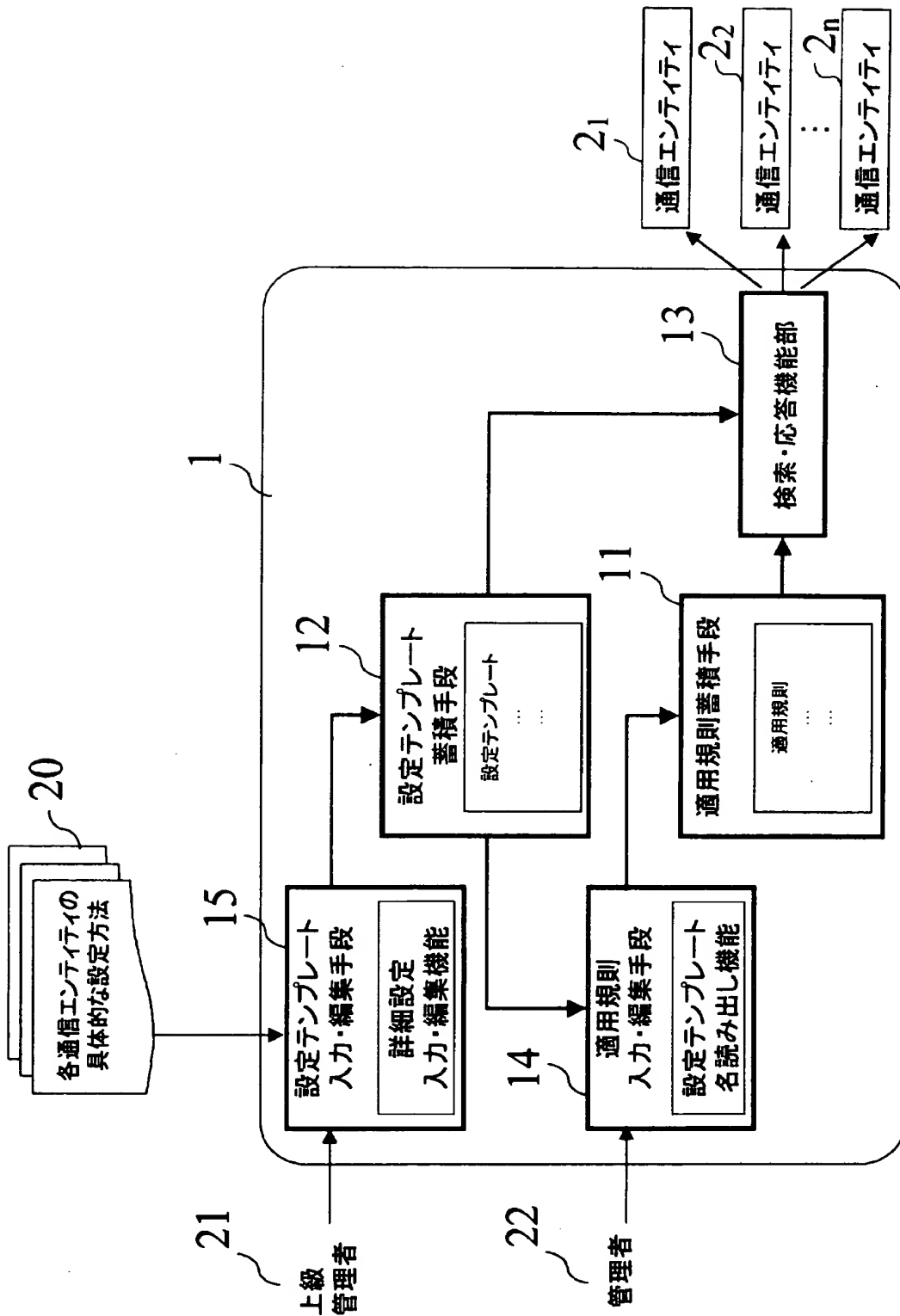
【図 2】



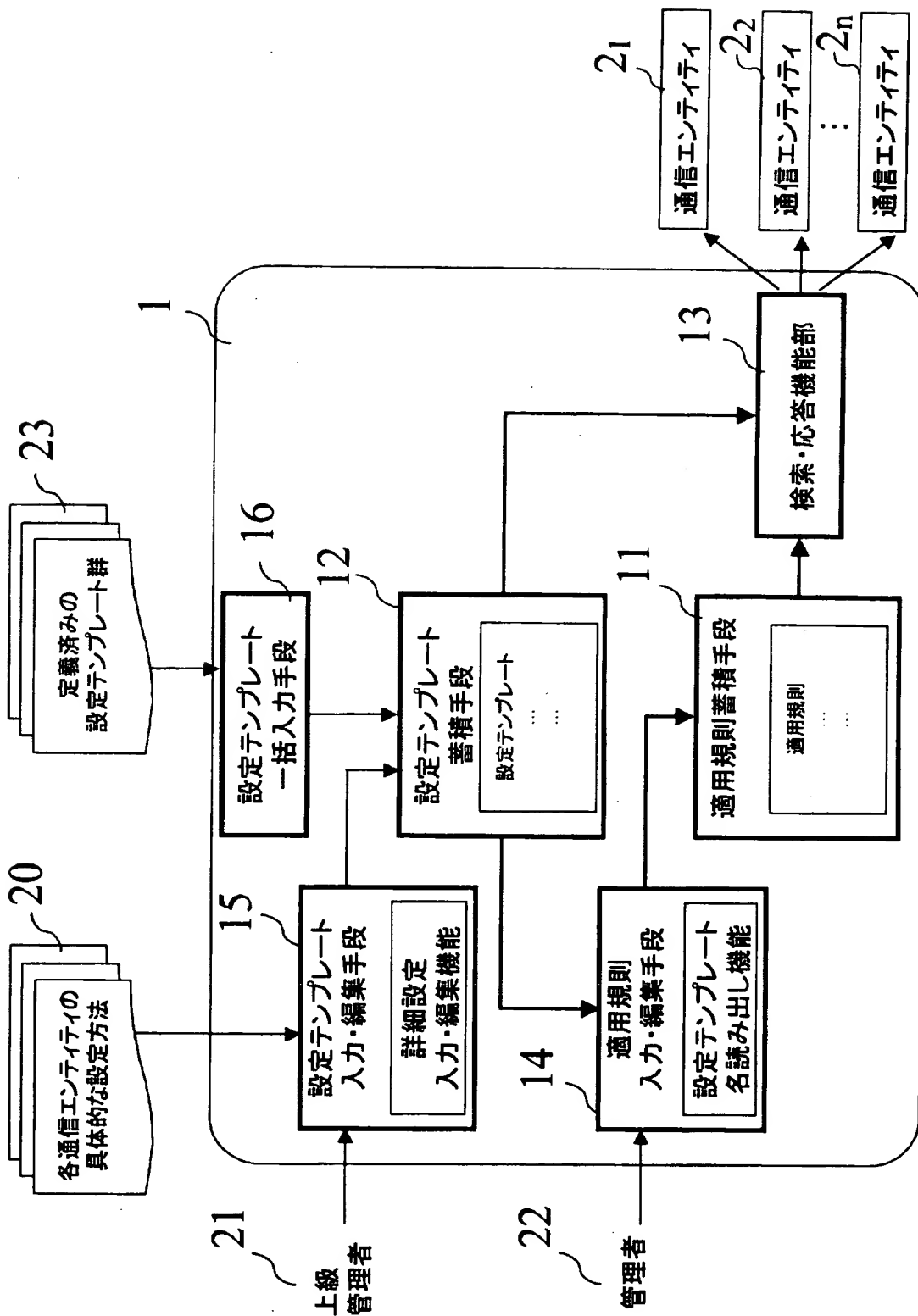
【図 3】



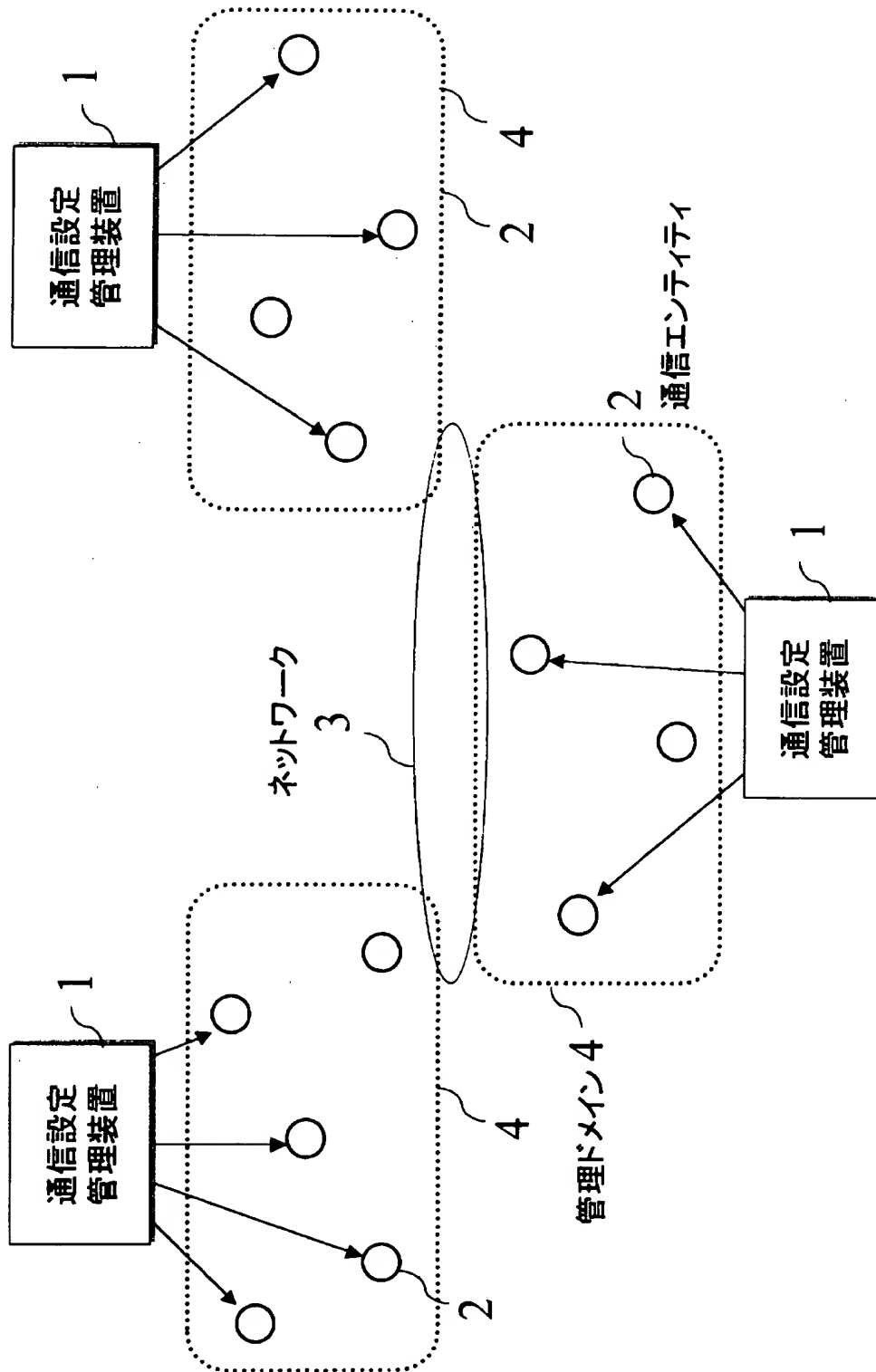
【図 4】



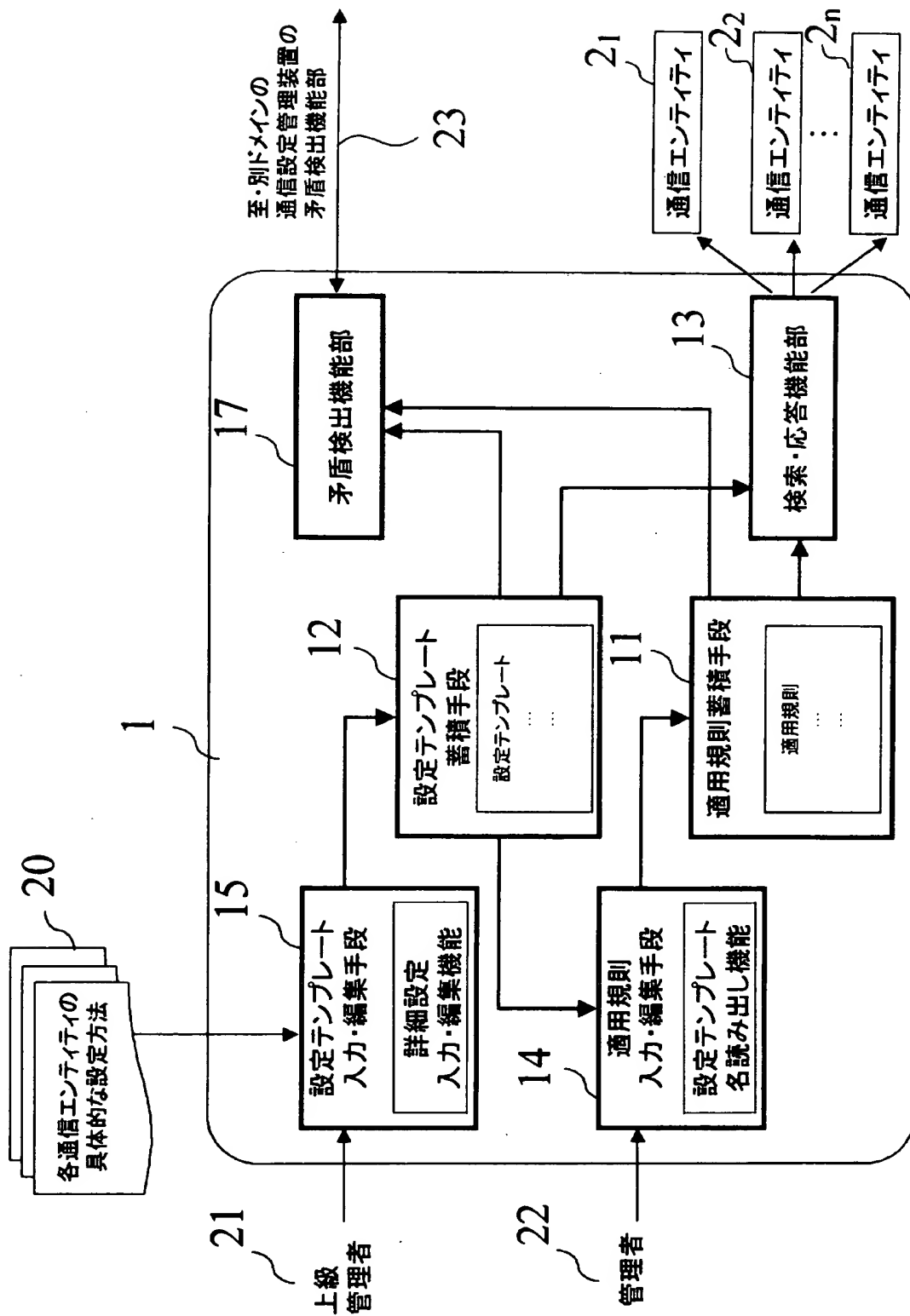
【図 5】



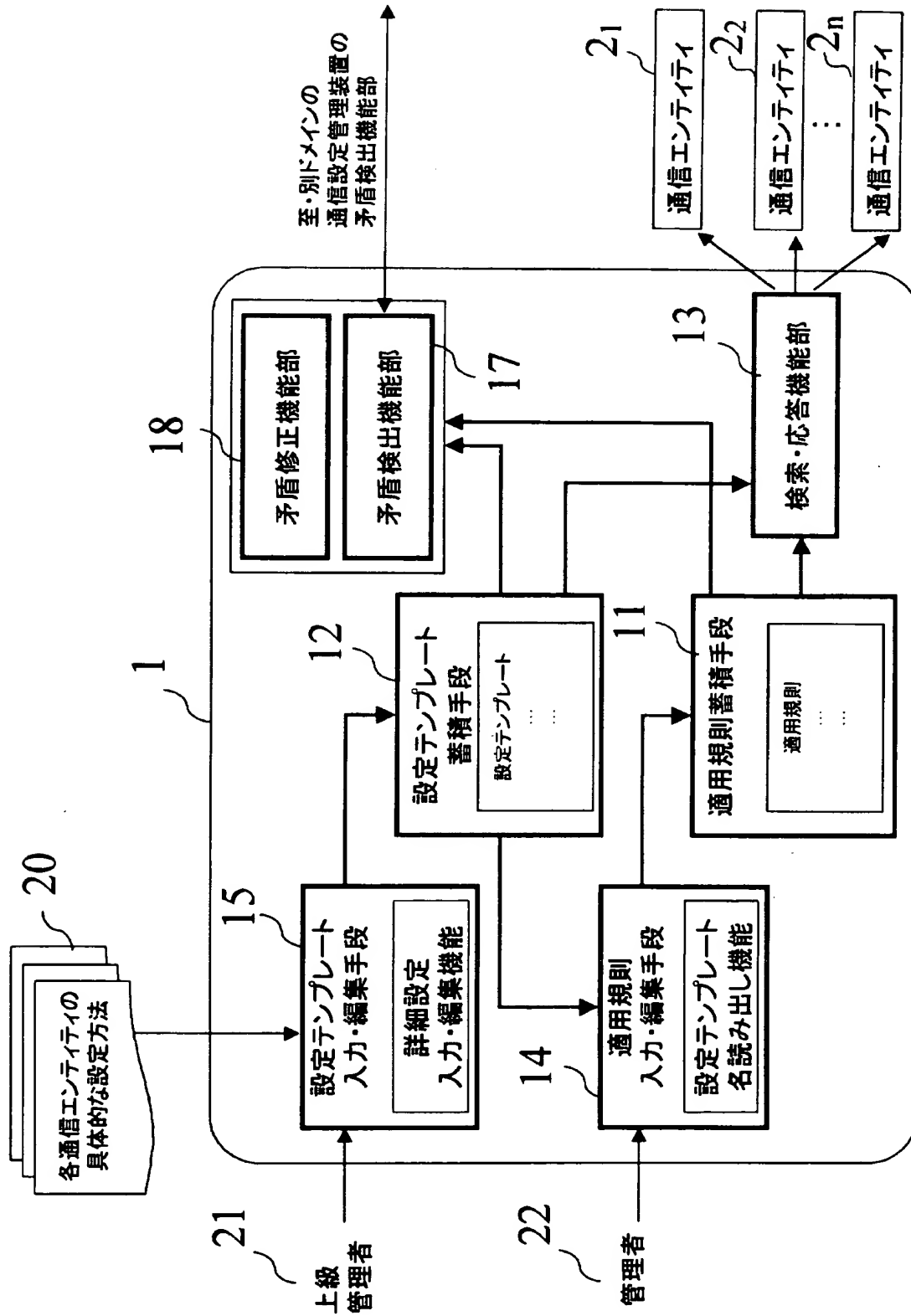
【図6】



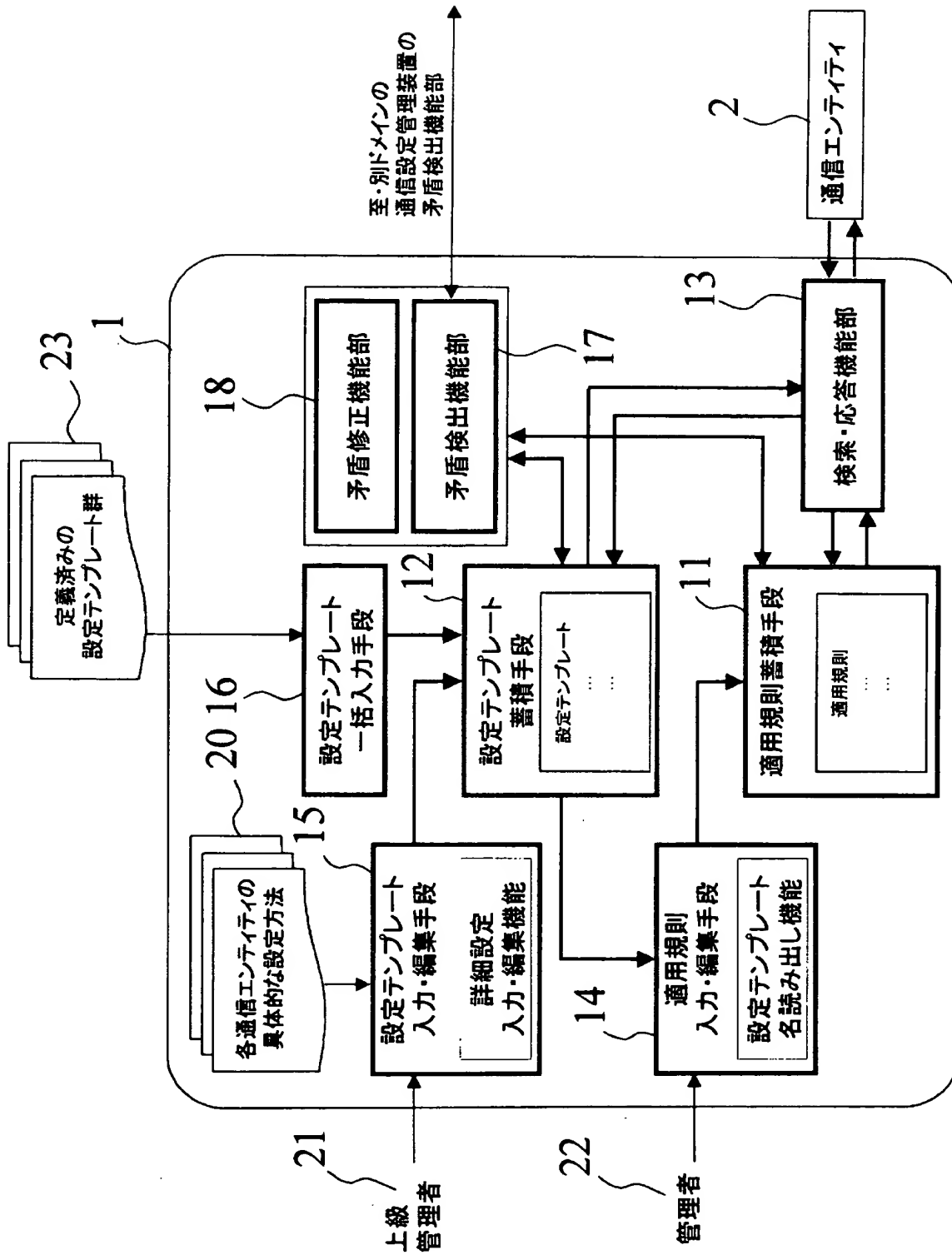
【図 7】



【図 8】



【図 9】



【図 1 0】

設定方法 20		
認証 200	秘匿 201	ログ記録 202
なし	なし	なし
RSA 512 bit	DES	あり
RSA 1024 bit	Triple DES	
RSA 2048 bit		

【図 1 1】

設定テンプレート名 210	コメント 211	設定内容 211		
		認証 200	秘匿 201	ログ記録 202
T00	セキュリティなし	なし	なし	なし
T01	人事情報用、ログなし	RSA 512 bit	DES	なし
T02	人事情報用、ログあり	RSA 512 bit	DES	あり
T03	取引先との通信用	RSA 1024 bit	Triple DES	あり

【図 1 2】

番号	subject 220	action 221	object 222	設定テンプレート名 210
1	Admin	read	人事情報サーバ	T01
2	Admin	write	人事情報サーバ	T02
3	Customer	read	公開サーバ	T00
4	Customer	read	顧客情報サーバ	T03
5	User	read	一般サーバ	T00
6	User	read	人事情報サーバ	T02

【図 1 3】

設定テンプレート入力・編集(新テンプレート追加中)

設定テンプレート名 210	コメント 212	設定内容 211		
		認証 200	秘匿 201	ログ記録 202
T00	セキュリティなし	なし	なし	なし
T01	人事情報用、ログなし	RSA 512 bit	DES	なし
T02	人事情報用、ログあり	RSA 512 bit	DES	あり
T03	取引先との通信用	RSA 1024 bit	Triple DES	あり
T04	関係会社との図面やりとり用	<div>なし RSA 512 bit RSA 1024 bit RSA 2048 bit</div>		

選択肢が示される

【図 1 4】

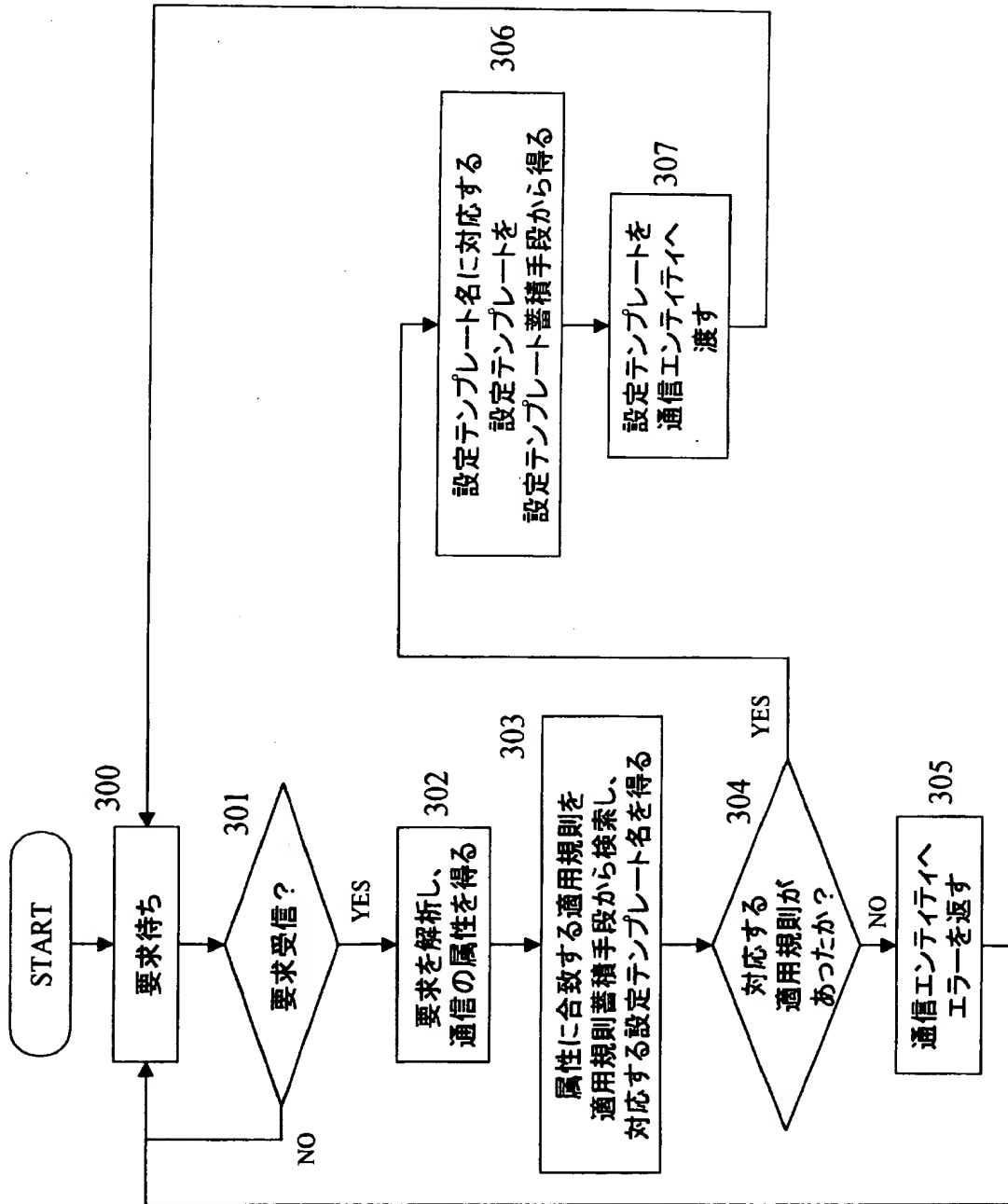
適用規則(新規適用規則追加中)

番号	subject 220	action 221	object 222	設定テンプレート名 210
1	Admin	read	人事情報サーバ	T01
2	Admin	write	人事情報サーバ	T02
3	Customer	read	公開サーバ	T00
4	Customer	read	顧客情報サーバ	T03
5	User	read	一般サーバ	T00
6	User	read	人事情報サーバ	T02
7	Ex_staff	read	設計図面サーバ	

選択肢が示される

T00: セキュリティなし
T01: 人事情報用、ログなし
T02: 人事情報用、ログあり
T03: 取引先との通信用
T04: 関係会社との図面やりとり用

【図 15】



【図 1 6】

A

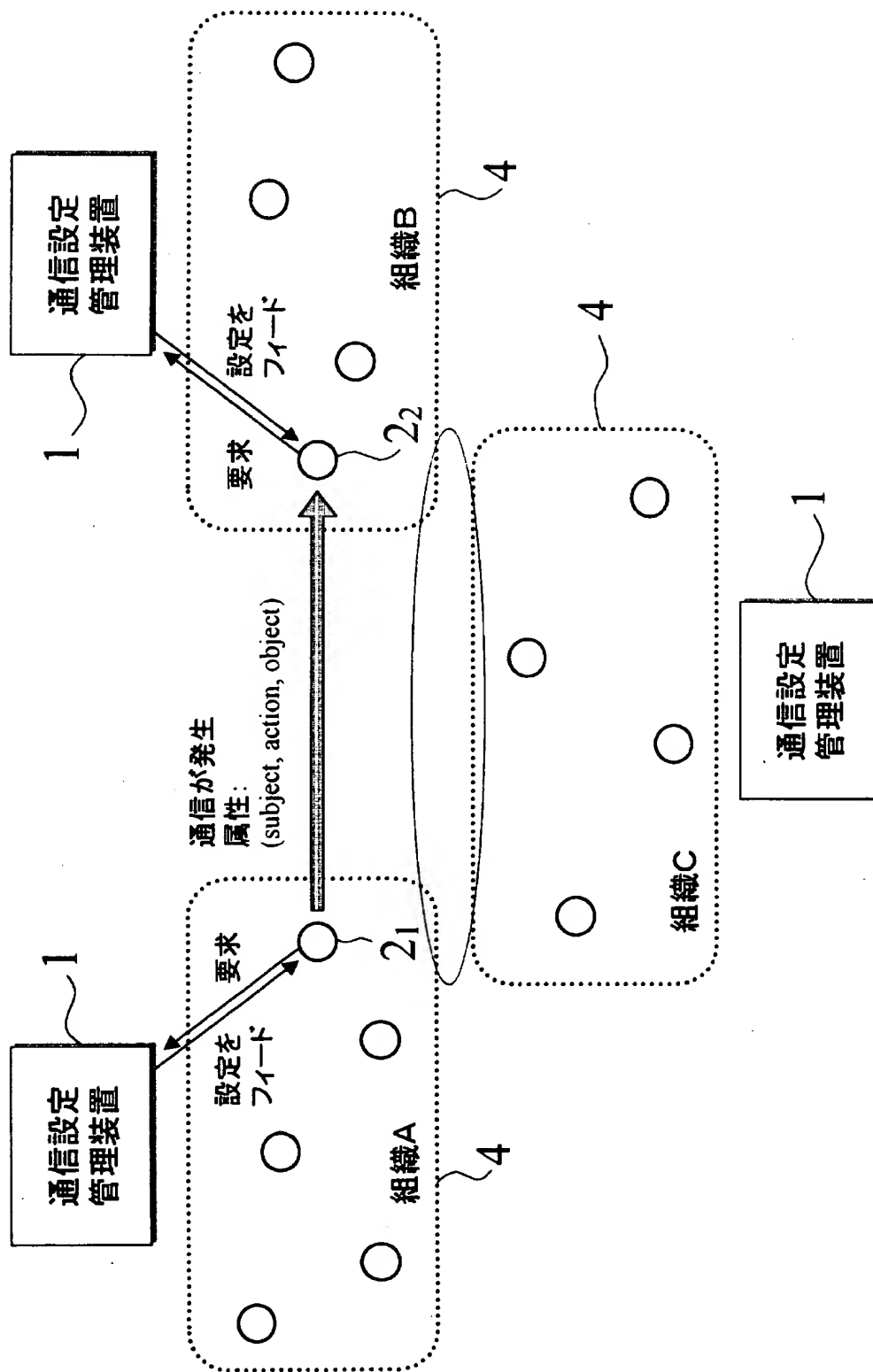
設定テンプレート名 210	コメント 212	設定内容 211		
		認証 200	秘匿 201	ログ記録 202
T11	人事情報用、ログなし(RC4)	RSA 512 bit	RC4	なし
T12	人事情報用、ログあり(RC4)	RSA 512 bit	RC4	あり
T13	取引先との通信用(RC4)	RSA 1024 bit	RC4	あり

B

設定内容 211			
認証	秘匿	ログ記録	
なし	なし	なし	
RSA 512 bit	DES	あり	
RSA 1024 bit	Triple DES		
RSA 2048 bit	RC4		

この項目を追加

【図17】



【図 1 8】

設定テンプレート名 210	コメント 212	設定内容 211		
		認証 200	秘匿 201	ログ記録 202
T21	セキュリティなし	なし	なし	なし
T22	ログ記録のみ	なし	なし	あり
T23	弱い暗号化	RSA 512 bit	DES	なし
T24	強い暗号化	RSA 512 bit	Triple DES	なし

【図 1 9】

組織Aの適用規則

A

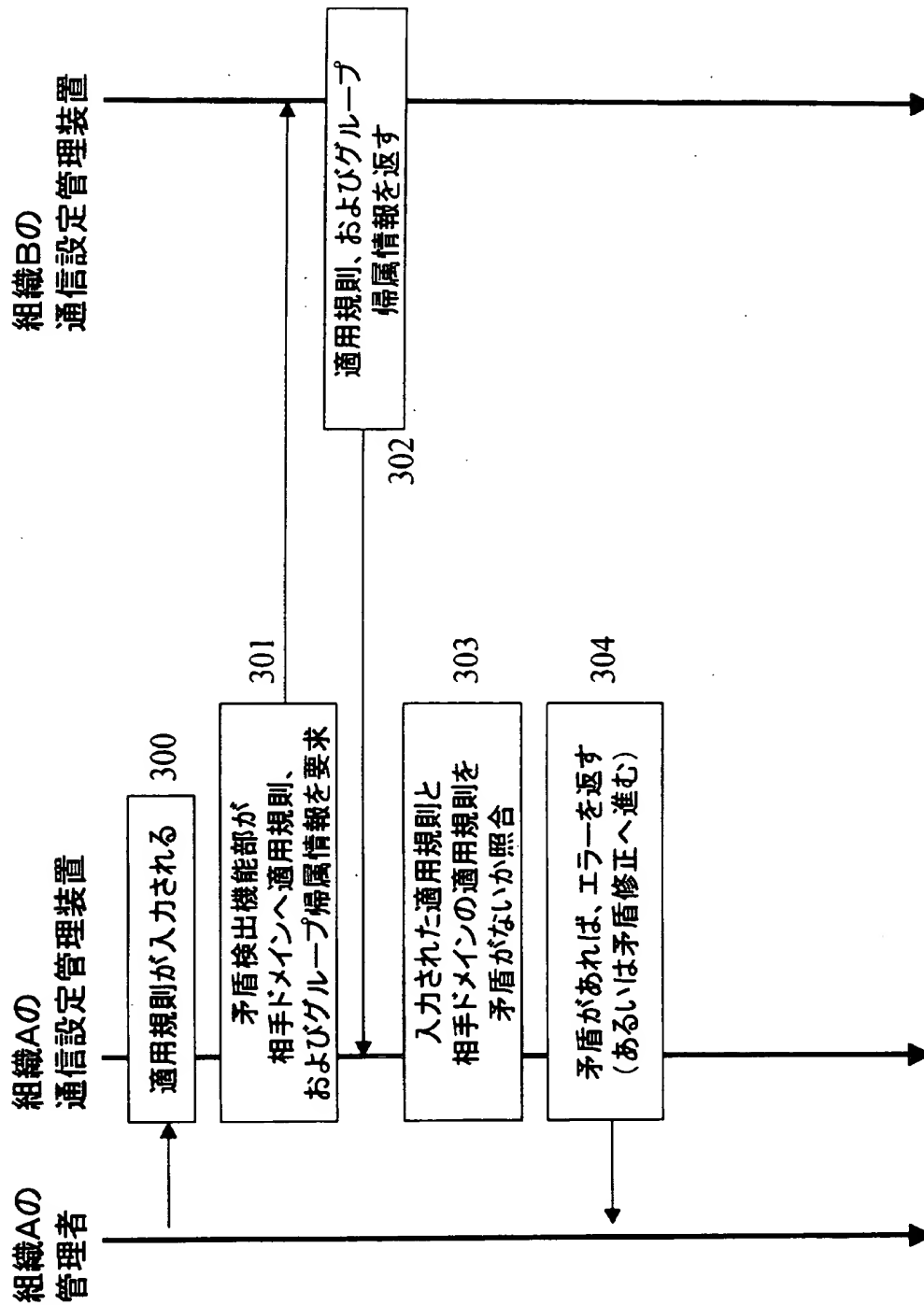
番号	subject	220	action	221	object	222	設定テンプレート名	220
1	User		read		一般サーバ		T21	31
2	User		read		人事情報サーバ		T23	32

組織Bの適用規則

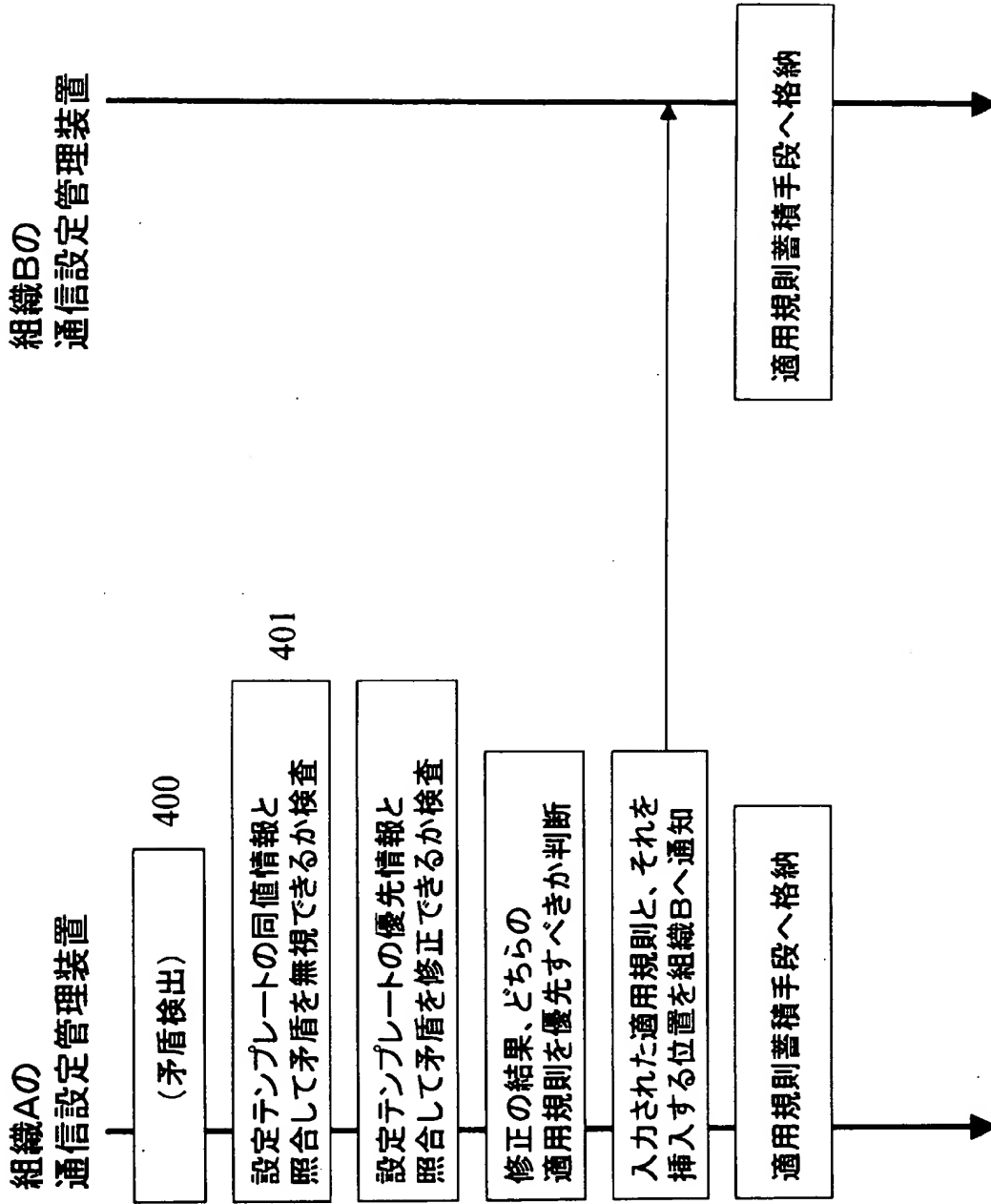
B

番号	subject	220	action	221	object	222	設定テンプレート名	220
1	User		read		一般サーバ		T22	41
2	SectionA		read		人事情報サーバ		T24	42

【図 2 0】



【図 2 1】



【図 2 2】

同値情報

A

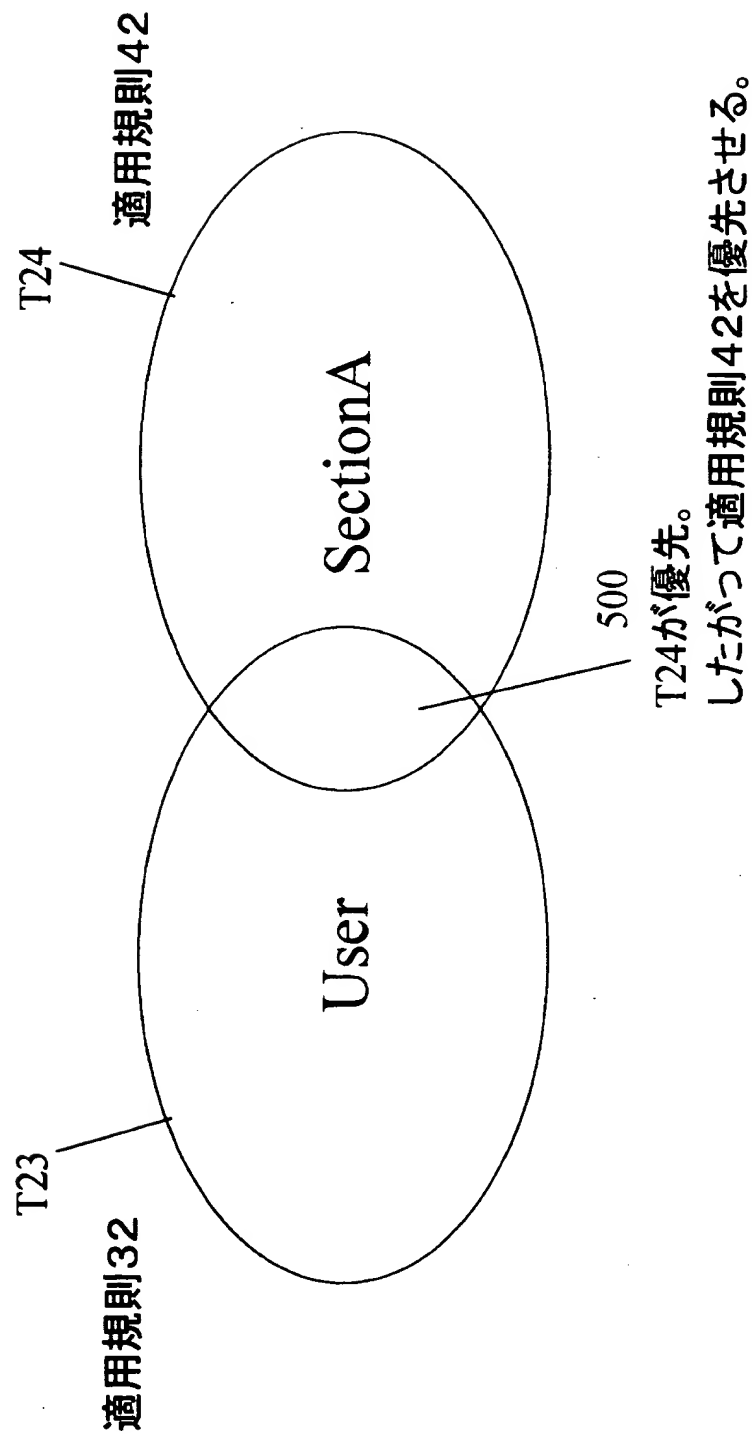
$$T21 = T22$$

優先情報

B

$$T23 < T24$$

【図 2 3】



【図 2 4】

組織Aの適用規則

番号	subject	action	object	設定テンプレート名
1	User	read	一般サーバ	T21 31
2	SectionA	read	人事情報サーバ	
3	User	read	人事情報サーバ	T23 32

組織Bの適用規則

番号	subject	action	object	設定テンプレート名
1	User	read	一般サーバ	T22 41
2	SectionA	read	人事情報サーバ	
3	User	read	人事情報サーバ	T23 42

【書類名】 要約書

【要約】

【課題】 通信設定を多くの通信エンティティへ配布する場合において、高度の知識を要するきめ細かな通信設定の記述と高度の知識を要さない容易な適用規則の記述が同時に実現できる通信設定管理システムを提供する。

【解決手段】 通信エンティティの具体的な設定方法の情報を参照して、通信エンティティに対し設定する内容を纏めた設定テンプレートを、入力又は編集する設定テンプレート入力・編集手段と、設定テンプレート入力・編集手段により入力又は編集された設定テンプレートを蓄積する設定テンプレート蓄積手段と、どのような属性を持った通信にどの設定テンプレートを適用すべきかの規則を記した適用規則を入力又は編集する適用規則入力・編集手段と、適用規則入力・編集手段により入力又は編集された適用規則を蓄積する適用規則蓄積手段と、設定を配布する先の通信エンティティの属性に従って、前記適用規則蓄積手段から該当する適用規則を選び、該適用規則で指定される設定テンプレート名を有する設定テンプレートを前記設定テンプレート蓄積手段から読み出し、該読み出された設定テンプレートを前記通信エンティティに配布を行う検索・応答機能手段を備える。

【選択図】 図 4

認定・付加情報

特許出願の番号	特願 2 0 0 0 - 1 4 5 6 4 6
受付番号	5 0 0 0 0 6 1 0 4 0 3
書類名	特許願
担当官	塩崎 博子 1 6 0 6
作成日	平成 1 2 年 5 月 3 1 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】	富士通株式会社

【特許出願人】

【識別番号】	500224324
【住所又は居所】	ドイツ連邦共和国 D-53757 サнкт オーガスティン
【氏名又は名称】	ゲーエムデー フォルシュンクスツェントルム インフォルマチオンテクニク ゲーエムペーハ ー

【代理人】

申請人

【識別番号】	100094514
【住所又は居所】	神奈川県横浜市港北区新横浜 3-9-5 第三東 昇ビル 3 階 林・土井 国際特許事務所
【氏名又は名称】	林 恒徳

【代理人】

【識別番号】	100094525
【住所又は居所】	神奈川県横浜市港北区新横浜 3-9-5 第三東 昇ビル 3 階 林・土井 国際特許事務所
【氏名又は名称】	土井 健二

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号

氏 名 富士通株式会社

出 願 人 履 歴 情 報

識別番号 [500224324]

1. 変更年月日 2000年 5月17日

[変更理由] 新規登録

住 所 ドイツ連邦共和国 D-53757 サンクト オーガスティ
ン

氏 名 ゲーエムデー フォルシュンクスツェントルム インフォルマ
チオンテクニック ゲーエムペーハー